

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-161935

(43) 公開日 平成10年(1998) 6月19日

(51) Int.Cl. <sup>6</sup>	識別記号	F I		
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B	
15/00	3 3 0	15/00	3 3 0 A	
H 0 4 Q 7/34		H 0 4 B 7/26	1 0 6 A	
7/38			1 0 9 R	
H 0 4 L 9/10		H 0 4 L 9/00	6 2 1 Z	
審査請求 未請求 請求項の数12 O L (全 30 頁) 最終頁に続く				

(21) 出願番号 特願平9-232934

(22) 出願日 平成9年(1997) 8月28日

(31) 優先権主張番号 特願平8-248244

(32) 優先日 平8(1996) 9月19日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 島川 和典

東京都青梅市末広町2丁目9番地 株式会

社東芝青梅工場内

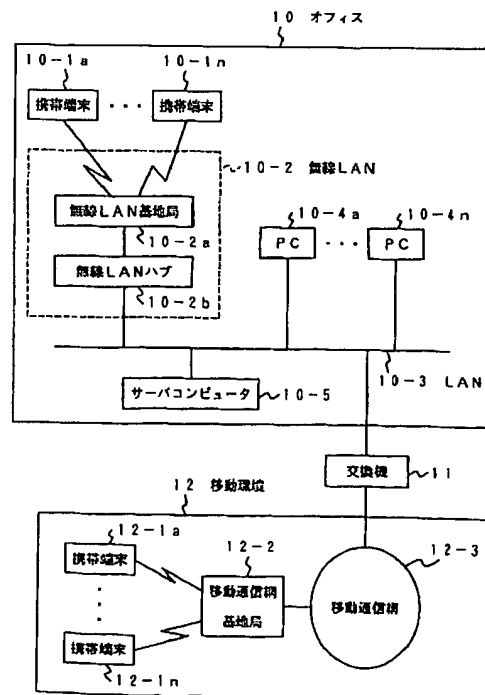
(74) 代理人 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 セキュリティシステム及びセキュリティ方法

(57) 【要約】

【課題】 携帯端末上のデータの暗号化／復号化を簡単に行うことができ、操作者に負担を掛けることなく、また、利便性に欠くことなくデータを保護する。

【解決手段】 携帯端末10-1aは非暗号データ記憶用メモリと暗号データ記憶用メモリを有する。オフィス10から移動環境12に移動するとき、操作者によって指定された暗号キーに従って非暗号データ記憶用メモリの非暗号データを暗号化する。この暗号化データを暗号データ記憶用メモリに書き込み、データのアクセス対象を暗号データ記憶用メモリとして暗号モードを設定する。一方、移動環境12からオフィス10に戻るとき、操作者によって指定された復号キーに従って暗号データ記憶用メモリの暗号データを復号化する。この復号化データつまり非暗号データを非暗号データ記憶用メモリに書き込み、データのアクセス対象を非暗号データ記憶用メモリとして暗号モードを設定する。



## 【特許請求の範囲】

【請求項1】 オフィスまたは移動環境で使用され、非暗号データを記憶するための非暗号データ記憶手段と暗号データを記憶するための暗号データ記憶手段とを有する携帯端末と、

この携帯端末を上記オフィスから上記移動環境に移動させるとき、暗号キーを指定する暗号キー指定手段と、

この暗号キー指定手段によって指定された上記暗号キーに従って上記非暗号データ記憶手段から上記非暗号データを読み出し、これを暗号化する暗号化手段と、

この暗号化手段によって暗号化されたデータを上記暗号データ記憶手段に書き込み、データのアクセス対象を上記暗号データ記憶手段として暗号モードを設定する暗号モード設定手段と、

上記携帯端末を上記移動環境から上記オフィスに移動させるとき、復号キーを指定する復号キー指定手段と、

この復号キー指定手段によって指定された上記復号キーに従って上記暗号データ記憶手段から上記暗号データを読み出し、これを復号化する復号化手段と、

この復号化手段によって復号化されたデータを上記非暗号データ記憶手段に書き込み、データのアクセス対象を上記非暗号データ記憶手段として非暗号モードを設定する非暗号モード設定手段とを具備したことを特徴とするセキュリティシステム。

【請求項2】 ネットワークに共有化または非共有化され、非暗号データを記憶するための非暗号データ記憶手段と暗号データを記憶するための暗号データ記憶手段とを有する携帯端末と、

この携帯端末をネットワークに非共有化するとき、暗号キーを指定する暗号キー指定手段と、

この暗号キー指定手段によって指定された上記暗号キーに従って上記非暗号データ記憶手段から上記非暗号データを読み出し、これを暗号化する暗号化手段と、

この暗号化手段によって暗号化されたデータを上記暗号データ記憶手段に書き込み、データのアクセス対象を上記暗号データ記憶手段として暗号モードを設定する暗号モード設定手段と、

上記携帯端末をネットワークに共有化するとき、復号キーを指定する復号キー指定手段と、

この復号キー指定手段によって指定された上記復号キーに従って上記暗号データ記憶手段から上記暗号データを読み出し、これを復号化する復号化手段と、

この復号化手段によって復号化されたデータを上記非暗号データ記憶手段に書き込み、データのアクセス対象を上記非暗号データ記憶手段として非暗号モードを設定する非暗号モード設定手段とを具備したことを特徴とするセキュリティシステム。

【請求項3】 無線環境下でオフィスまたは移動環境で使用され、非暗号データを記憶するための非暗号データ記憶手段と暗号データを記憶するための暗号データ記憶

手段とを有する携帯端末と、

この携帯端末が受信する電波が上記オフィスに特有のものか上記移動環境に特有のものかを検出する電波検出手段と、

この電波検出手段によって上記移動環境に特有の電波が検出されたとき、暗号キーを指定する暗号キー指定手段と、

この暗号キー指定手段によって指定された上記暗号キーに従って上記非暗号データ記憶手段から上記非暗号データを読み出し、これを暗号化する暗号化手段と、

この暗号化手段によって暗号化されたデータを上記暗号データ記憶手段に書き込み、データのアクセス対象を上記暗号データ記憶手段として暗号モードを設定する暗号モード設定手段と、

上記電波検出手段によって上記オフィスに特有の電波が検出されたとき、復号キーを指定する復号キー指定手段と、

この復号キー指定手段によって指定された上記復号キーに従って上記暗号データ記憶手段から上記暗号データを読み出し、これを復号化する復号化手段と、

この復号化手段によって復号化されたデータを上記非暗号データ記憶手段に書き込み、データのアクセス対象を上記非暗号データ記憶手段として非暗号モードを設定する非暗号モード設定手段とを具備したことを特徴とするセキュリティシステム。

【請求項4】 無線環境下でオフィスまたは移動環境で使用されると共に、ネットワークに共有化または非共有化され、非暗号データを記憶するための非暗号データ記憶手段と暗号データを記憶するための暗号データ記憶手段とを有する携帯端末と、

この携帯端末が受信する電波が上記オフィスに特有のものか上記移動環境に特有のものかを検出する電波検出手段と、

この電波検出手段によって上記移動環境に特有の電波が検出されたとき、あるいは、上記携帯端末をネットワークに非共有化するとき、暗号キーを指定する暗号キー指定手段と、

この暗号キー指定手段によって指定された上記暗号キーに従って上記非暗号データ記憶手段から上記非暗号データを読み出し、これを暗号化する暗号化手段と、

この暗号化手段によって暗号化されたデータを上記暗号データ記憶手段に書き込み、データのアクセス対象を上記暗号データ記憶手段として暗号モードを設定する暗号モード設定手段と、

上記電波検出手段によって上記オフィスに特有の電波が検出されたとき、あるいは、上記携帯端末をネットワークに共有化するとき、復号キーを指定する復号キー指定手段と、

この復号キー指定手段によって指定された上記復号キーに従って上記暗号データ記憶手段から上記暗号データを

読み出し、これを復号化する復号化手段と、

この復号化手段によって復号化されたデータを上記非暗号データ記憶手段に書き込み、データのアクセス対象を上記非暗号データ記憶手段として非暗号モードを設定する非暗号モード設定手段とを具備したことを特徴とするセキュリティシステム。

【請求項5】 オフィスまたは移動環境で使用され、非暗号データを記憶するための非暗号データ記憶用メモリと暗号データを記憶するための暗号データ記憶用メモリとを有する携帯端末に対するセキュリティ方法であつて、

この携帯端末を上記オフィスから上記移動環境に移動させるとき、暗号キーを指定し、

この指定された上記暗号キーに従って上記非暗号データ記憶用メモリから上記非暗号データを読み出し、これを暗号化した後、

この暗号化されたデータを上記暗号データ記憶用メモリに書き込み、データのアクセス対象を上記暗号データ記憶用メモリとして暗号モードを設定し、

上記携帯端末を上記移動環境から上記オフィスに移動させるとき、復号キーを指定し、

この指定された上記復号キーに従って上記暗号データ記憶用メモリから上記暗号データを読み出し、これを復号化した後、

この暗号化手段によって暗号化されたデータを上記暗号データ記憶用メモリに書き込み、データのアクセス対象を上記非暗号データ記憶用メモリとして非暗号モードを設定するようにしたことを特徴とするセキュリティ方法。

【請求項6】 ネットワークに共有化または非共有化され、非暗号データを記憶するための非暗号データ記憶用メモリと暗号データを記憶するための暗号データ記憶用メモリとを有する携帯端末に対するセキュリティ方法であつて、

この携帯端末をネットワークに非共有化するとき、暗号キーを指定し、

この指定された上記暗号キーに従って上記非暗号データ記憶用メモリから上記非暗号データを読み出し、これを暗号化した後、

この暗号化されたデータを上記暗号データ記憶用メモリに書き込み、データのアクセス対象を上記暗号データ記憶用メモリとして暗号モードを設定し、

上記携帯端末をネットワークに共有化するとき、復号キーを指定し、

この指定された上記復号キーに従って上記暗号データ記憶用メモリから上記暗号データを読み出し、これを復号化した後、

この復号化されたデータを上記非暗号データ記憶用メモリに書き込み、データのアクセス対象を上記非暗号データ記憶用メモリとして非暗号モードを設定するようにし

たことを特徴とするセキュリティ方法。

【請求項7】 無線環境下でオフィスまたは移動環境で使用され、非暗号データを記憶するための非暗号データ記憶用メモリと暗号データを記憶するための暗号データ記憶用メモリとを有する携帯端末に対するセキュリティ方法であつて、

この携帯端末が受信する電波が上記オフィスに特有のものか上記移動環境に特有のものを検出し、

上記移動環境に特有の電波が検出されたとき、暗号キーを指定し、

この指定された上記暗号キーに従って上記非暗号データ記憶用メモリから上記非暗号データを読み出し、これを暗号化した後、

この暗号化されたデータを上記暗号データ記憶用メモリに書き込み、データのアクセス対象を上記暗号データ記憶用メモリとして暗号モードを設定し、

上記オフィスに特有の電波が検出されたとき、復号キーを指定し、

この指定された上記復号キーに従って上記暗号データ記憶用メモリから上記暗号データを読み出し、これを復号化した後、

この復号化されたデータを上記非暗号データ記憶用メモリに書き込み、データのアクセス対象を上記非暗号データ記憶用メモリとして非暗号モードを設定するようにしたことを特徴とするセキュリティ方法。

【請求項8】 無線環境下でオフィスまたは移動環境で使用されると共に、ネットワークに共有化または非共有化され、非暗号データを記憶するための非暗号データ記憶用メモリと暗号データを記憶するための暗号データ記憶用メモリとを有する携帯端末に対するセキュリティ方法であつて、

この携帯端末が受信する電波が上記オフィスに特有のものか上記移動環境に特有のものを検出し、

上記移動環境に特有の電波が検出されたとき、あるいは、上記携帯端末をネットワークに非共有化するとき、暗号キーを指定し、

この指定された上記暗号キーに従って上記非暗号データ記憶用メモリから上記非暗号データを読み出し、これを暗号化した後、

この暗号化されたデータを上記暗号データ記憶用メモリに書き込み、データのアクセス対象を上記暗号データ記憶用メモリとして暗号モードを設定し、

上記オフィスに特有の電波が検出されたとき、あるいは、上記携帯端末をネットワークに共有化するとき、復号キーを指定し、

この指定された上記復号キーに従って上記暗号データ記憶用メモリから上記暗号データを読み出し、これを復号化した後、

この復号化されたデータを上記非暗号データ記憶用メモリに書き込み、データのアクセス対象を上記非暗号デー

10

20

30

40

50

## 5

タ記憶用メモリとして非暗号モードを設定するようにしたことを特徴とするセキュリティ方法。

【請求項9】 オフィスまたは移動環境で使用され、非暗号データを記憶するための非暗号データ記憶用メモリと暗号データを記憶するための暗号データ記憶用メモリとを有する携帯端末に対するセキュリティを実現するためのプログラムであって、

この携帯端末を上記オフィスから上記移動環境に移動させるとき、暗号キーを指定し、

この指定された上記暗号キーに従って上記非暗号データ記憶用メモリから上記非暗号データを読み出し、これを暗号化した後、

この暗号化されたデータを上記暗号データ記憶用メモリに書き込み、データのアクセス対象を上記暗号データ記憶用メモリとして暗号モードを設定し、

上記携帯端末を上記移動環境から上記オフィスに移動させるとき、復号キーを指定し、

この指定された上記復号キーに従って上記暗号データ記憶用メモリから上記暗号データを読み出し、これを復号化した後、

この暗号化手段によって暗号化されたデータを上記暗号データ記憶用メモリに書き込み、データのアクセス対象を上記非暗号データ記憶用メモリとして非暗号モードを設定するようにコンピュータを制御するためのプログラムを格納したコンピュータ読取可能な記憶媒体。

【請求項10】 ネットワークに共有化または非共有化され、非暗号データを記憶するための非暗号データ記憶用メモリと暗号データを記憶するための暗号データ記憶用メモリとを有する携帯端末に対するセキュリティを実現するためのプログラムであって、

この携帯端末をネットワークに非共有化するとき、暗号キーを指定し、

この指定された上記暗号キーに従って上記非暗号データ記憶用メモリから上記非暗号データを読み出し、これを暗号化した後、

この暗号化されたデータを上記暗号データ記憶用メモリに書き込み、データのアクセス対象を上記暗号データ記憶用メモリとして暗号モードを設定し、

上記携帯端末をネットワークに共有化するとき、復号キーを指定し、

この指定された上記復号キーに従って上記暗号データ記憶用メモリから上記暗号データを読み出し、これを復号化した後、

この復号化されたデータを上記非暗号データ記憶用メモリに書き込み、データのアクセス対象を上記非暗号データ記憶用メモリとして非暗号モードを設定するようにコンピュータを制御するためのプログラムを格納したコンピュータ読取可能な記憶媒体。

【請求項11】 無線環境下でオフィスまたは移動環境で使用され、非暗号データを記憶するための非暗号デー

## 6

タ記憶用メモリと暗号データを記憶するための暗号データ記憶用メモリとを有する携帯端末に対するセキュリティを実現するためのプログラムであって、

この携帯端末が受信する電波が上記オフィスに特有のものか上記移動環境に特有のものを検出し、

上記移動環境に特有の電波が検出されたとき、暗号キーを指定し、

この指定された上記暗号キーに従って上記非暗号データ記憶用メモリから上記非暗号データを読み出し、これを暗号化した後、

この暗号化されたデータを上記暗号データ記憶用メモリに書き込み、データのアクセス対象を上記暗号データ記憶用メモリとして暗号モードを設定し、

上記オフィスに特有の電波が検出されたとき、復号キーを指定し、

この指定された上記復号キーに従って上記暗号データ記憶用メモリから上記暗号データを読み出し、これを復号化した後、

この復号化されたデータを上記非暗号データ記憶用メモリに書き込み、データのアクセス対象を上記非暗号データ記憶用メモリとして非暗号モードを設定するようにコンピュータを制御するためのプログラムを格納したコンピュータ読取可能な記憶媒体。

【請求項12】 無線環境下でオフィスまたは移動環境で使用されると共に、ネットワークに共有化または非共有化され、非暗号データを記憶するための非暗号データ記憶用メモリと暗号データを記憶するための暗号データ記憶用メモリとを有する携帯端末に対するセキュリティを実現するためのプログラムであって、

この携帯端末が受信する電波が上記オフィスに特有のものか上記移動環境に特有のものを検出し、

上記移動環境に特有の電波が検出されたとき、あるいは、上記携帯端末をネットワークに非共有化するとき、暗号キーを指定し、

この指定された上記暗号キーに従って上記非暗号データ記憶用メモリから上記非暗号データを読み出し、これを暗号化した後、

この暗号化されたデータを上記暗号データ記憶用メモリに書き込み、データのアクセス対象を上記暗号データ記憶用メモリとして暗号モードを設定し、

上記オフィスに特有の電波が検出されたとき、あるいは、上記携帯端末をネットワークに共有化するとき、復号キーを指定し、

この指定された上記復号キーに従って上記暗号データ記憶用メモリから上記暗号データを読み出し、これを復号化した後、

この復号化されたデータを上記非暗号データ記憶用メモリに書き込み、データのアクセス対象を上記非暗号データ記憶用メモリとして非暗号モードを設定するようにコンピュータを制御するためのプログラムを格納したコン

ピュータ読取可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、携帯端末で扱うデータのセキュリティを保証するセキュリティシステムに係り、特にオフィスと移動環境とでデータの暗号化／復号化を効率的に行うことでセキュリティを保証するセキュリティシステム及びセキュリティ方法に関する。

【0002】

【従来の技術】従来、例えばPDA (personal digital assistants) のような携帯端末にPHS (personal handyphone system) 等の通信機能を備えたものがある。このような携帯端末を持ち歩くことにより、オフィス内はもちろんのこと、オフィス外であってもデータを取り扱うことができる。また、オフィス外であっても、オフィス内に設置されたホストコンピュータ等とデータ通信を行うこともできる。

【0003】ところで、オフィス外の市街地や、電車などの移動環境にて携帯端末を使用する場合には、置き忘れや盗難などにより携帯端末上のデータが漏洩の危険にさらされるという問題がある。このような問題に対しては、例えばデータの暗号化、携帯端末へのログインによるユーザ認証、ICカードに記録された復号キーを用いた復号化など、種々の方式が実現されている。

【0004】しかしながら、これらの方式の欠点は携帯端末を使う場所を操作者自ら意識してデータを暗号化しなければならないということである。すなわち、オフィスから移動環境への移動に際しては、オフィス内にある個人専用のパーソナルコンピュータ(PC)や、グループで共有して使用するサーバコンピュータ上のデータ(ファイル)をその都度暗号化して携帯端末にコピーする、といった作業を忘れずに行う必要がある。

【0005】なお、常にデータを暗号化するという方法もあるが、一般にオフィス内では暗号化は不要であり、また、そのような暗号化されたデータを使用する場合にはその都度復号化を必要とするため、利便性に欠けるといった問題がある。

【0006】

【発明が解決しようとする課題】上述したように、従来、携帯端末の置き忘れや、盗難などによってデータが漏洩してしまうことを防止するためには、オフィス内にあるコンピュータのデータを取り出す際に、それを暗号化して、携帯端末にコピーするといった作業を行う必要があった。

【0007】この場合、オフィスと移動環境との間を行き来する場合には、その場所がオフィス内であればデータを暗号化せず、移動環境であればデータを暗号化する、といったように移動場所に応じて適宜暗号化の作業を必要とし、また、暗号化されたデータを復号化する作業も必要となることから、携帯端末を使用する操作者に

負担を掛けると同時に利便性に欠けるという問題があった。

【0008】また、従来では、操作者の判断によってデータの暗号化を適宜行う必要があった。このため、移動環境に移動する際に暗号化を怠る可能性が多々あり、データが漏洩しやすい等の問題があった。

【0009】本発明は上記のような点に鑑みなされたもので、携帯端末上のデータの暗号化／復号化を簡単に行うことができ、これにより、操作者に負担を掛けることなく、また、利便性に欠くことなくデータを保護することのできるセキュリティシステム及びセキュリティ方法を提供することを目的とする。

【0010】特に、本発明では、以下のような利便性の高いセキュリティシステム及びセキュリティ方法を提供することを目的とする。

【0011】(1) オフィスと移動環境間の移動時において、携帯端末上のデータをオフィスでは非暗号データ、移動環境では暗号データに適宜変換可能とする。

【0012】(2) ネットワーク上で共有化される携帯端末を使用する場合において、携帯端末上のデータを非共有化時には暗号データ、共有化時には非暗号データに適宜変換可能とする。

【0013】(3) 無線環境で携帯端末を使用する場合において、無線電波の種別に応じてオフィス／移動環境を自動的に判断し、携帯端末上のデータをオフィスでは非暗号データ、移動環境では暗号データに適宜変換可能とする。

【0014】(4) 無線環境で使用すると共にネットワーク上で共有化される携帯端末を使用する場合において、携帯端末上のデータをオフィスでは非暗号データ、移動環境では暗号データに適宜変換可能とし、さらに、非共有化時には暗号データ、共有化時には非暗号データに適宜変換可能とする。

【0015】

【課題を解決するための手段】

(1) 本発明のセキュリティシステムは、オフィスまたは移動環境で使用され、非暗号データを記憶するための非暗号データ記憶手段と暗号データを記憶するための暗号データ記憶手段とを有する携帯端末と、この携帯端末を上記オフィスから上記移動環境に移動させるとき、暗号キーを指定する暗号キー指定手段と、この暗号キー指定手段によって指定された上記暗号キーに従って上記非暗号データ記憶手段から上記非暗号データを読み出し、これを暗号化する暗号化手段と、この暗号化手段によって暗号化されたデータを上記暗号データ記憶手段に書き込み、データのアクセス対象を上記暗号データ記憶手段として暗号モードを設定する暗号モード設定手段と、上記携帯端末を上記移動環境から上記オフィスに移動させるとき、復号キーを指定する復号キー指定手段と、この復号キー指定手段によって指定された上記復号キーに従

って上記暗号データ記憶手段から上記暗号データを読み出し、これを復号化する復号化手段と、この復号化手段によって復号化されたデータを上記非暗号データ記憶手段に書き込み、データのアクセス対象を上記非暗号データ記憶手段として非暗号モードを設定する非暗号モード設定手段とを具備したものである。

【0016】このような構成によれば、携帯端末をオフィスから移動環境に移動させるとき、操作者により指定された暗号キーに従って携帯端末上の非暗号データが暗号化され、その暗号データをアクセス対象とするような暗号モードが設定される。一方、携帯端末を移動環境からオフィスに移動させるとき、操作者により指定された復号キーに従って暗号データが復号化され、その復号データつまり非暗号データをアクセス対象とするような非暗号モードが設定される。

【0017】このように、オフィスから移動環境に移動するときには、操作者が指定した暗号キーに従って携帯端末上のデータを暗号化して持ち歩くことができる。これにより、移動環境において、盗難や置き忘れなどによってデータが漏洩してしまうのを防ぐことができる。一方、移動環境からオフィスに戻るときには、操作者が指定した暗号キーに従って、その暗号データを復号化して元に戻すことができる。これにより、オフィス内では、常に誰もがデータを確認することができる。

【0018】(2) また、本発明のセキュリティシステムは、ネットワークに共有化または非共有化され、非暗号データを記憶するための非暗号データ記憶手段と暗号データを記憶するための暗号データ記憶手段とを有する携帯端末と、この携帯端末をネットワークに非共有化するとき、暗号キーを指定する暗号キー指定手段と、この暗号キー指定手段によって指定された上記暗号キーに従って上記非暗号データ記憶手段から上記非暗号データを読み出し、これを暗号化する暗号化手段と、この暗号化手段によって暗号化されたデータを上記暗号データ記憶手段に書き込み、データのアクセス対象を上記暗号データ記憶手段として暗号モードを設定する暗号モード設定手段と、上記携帯端末をネットワークに共有化するとき、復号キーを指定する復号キー指定手段と、この復号キー指定手段によって指定された上記復号キーに従って上記暗号データ記憶手段から上記暗号データを読み出し、これを復号化する復号化手段と、この復号化手段によって復号化されたデータを上記非暗号データ記憶手段に書き込み、データのアクセス対象を上記非暗号データ記憶手段として非暗号モードを設定する非暗号モード設定手段とを具備したものである。

【0019】このような構成によれば、携帯端末をネットワークに非共有化するとき、操作者により指定された暗号キーに従って携帯端末上の非暗号データが暗号化され、その暗号データをアクセス対象とするような暗号モードが設定される。一方、携帯端末をネットワークに共

有化するとき、携帯端末を移動環境からオフィスに移動させるとき、操作者により指定された復号キーに従って暗号データが復号化され、その復号データつまり非暗号データをアクセス対象とするような非暗号モードが設定される。

【0020】このように、携帯端末上のデータをオフィスに設置されたネットワーク上で共有資源としてPCにより共有化している間は暗号データが復号化される。一方、非共有化したときには、データが暗号化されるといった柔軟でかつ安全性の高い携帯端末の利用を実現できる。これにより、移動環境に限らずオフィス内での盗難や置き忘れ時にもデータ保護ができる携帯端末を提供できる。

【0021】(3) また、本発明のセキュリティシステムは、無線環境下でオフィスまたは移動環境で使用され、非暗号データを記憶するための非暗号データ記憶手段と暗号データを記憶するための暗号データ記憶手段とを有する携帯端末と、この携帯端末が受信する電波が上記オフィスに特有のものか上記移動環境に特有のものかを検出する電波検出手段と、この電波検出手段によって上記移動環境に特有の電波が検出されたとき、暗号キーを指定する暗号キー指定手段と、この暗号キー指定手段によって指定された上記暗号キーに従って上記非暗号データ記憶手段から上記非暗号データを読み出し、これを暗号化する暗号化手段と、この暗号化手段によって暗号化されたデータを上記暗号データ記憶手段に書き込み、データのアクセス対象を上記暗号データ記憶手段として暗号モードを設定する暗号モード設定手段と、上記電波検出手段によって上記オフィスに特有の電波が検出されたとき、復号キーを指定する復号キー指定手段と、この復号キー指定手段によって指定された上記復号キーに従って上記暗号データ記憶手段から上記暗号データを読み出し、これを復号化する復号化手段と、この復号化手段によって復号化されたデータを上記非暗号データ記憶手段に書き込み、データのアクセス対象を上記非暗号データ記憶手段として非暗号モードを設定する非暗号モード設定手段とを具備したものである。

【0022】このような構成によれば、携帯端末が受信する電波がオフィスに特有のものか移動環境に特有のものかが検出される。移動環境に特有の電波が検出されたとき、操作者により指定された暗号キーに従って携帯端末上の非暗号データが暗号化され、その暗号データをアクセス対象とするような暗号モードが設定される。一方、オフィスに特有の電波が検出されたとき、操作者により指定された復号キーに従って暗号データが復号化され、その復号データつまり非暗号データをアクセス対象とするような非暗号モードが設定される。

【0023】このように、携帯端末の操作者が自分の存在する環境を意識することなく、電波環境の変化に応じて暗号化／復号化が自動的に行われる。これにより、操

作者が自分の存在する環境では不適切であり、結果として誤った暗号化または復号化の処理を実行するといった操作ミスをなくすることができる。

【0024】(4)また、本発明のセキュリティシステムは、無線環境下でオフィスまたは移動環境で使用されると共に、ネットワークに共有化または非共有化され、非暗号データを記憶するための非暗号データ記憶手段と暗号データを記憶するための暗号データ記憶手段とを有する携帯端末と、この携帯端末が受信する電波が上記オフィスに特有のものか上記移動環境に特有のものを検出する電波検出手段と、この電波検出手段によって上記移動環境に特有の電波が検出されたとき、あるいは、上記携帯端末をネットワークに非共有化するとき、暗号キーを指定する暗号キー指定手段と、この暗号キー指定手段によって指定された上記暗号キーに従って上記非暗号データ記憶手段から上記非暗号データを読み出し、これを暗号化する暗号化手段と、この暗号化手段によって暗号化されたデータを上記暗号データ記憶手段に書き込み、データのアクセス対象を上記暗号データ記憶手段として暗号モードを設定する暗号モード設定手段と、上記電波検出手段によって上記オフィスに特有の電波が検出されたとき、あるいは、上記携帯端末をネットワークに共有化するとき、復号キーを指定する復号キー指定手段と、この復号キー指定手段によって指定された上記復号キーに従って上記暗号データ記憶手段から上記暗号データを読み出し、これを復号化する復号化手段と、この復号化手段によって復号化されたデータを上記非暗号データ記憶手段に書き込み、データのアクセス対象を上記非暗号データ記憶手段として非暗号モードを設定する非暗号モード設定手段とを具備したものである。

【0025】このような構成によれば、移動環境に特有の電波が検出されたとき、あるいは、携帯端末をネットワークに非共有化するとき、操作者により指定された暗号キーに従って携帯端末上の非暗号データが暗号化され、その暗号データをアクセス対象とするような暗号モードが設定される。一方、オフィスに特有の電波が検出されたとき、あるいは、携帯端末をネットワークに共有化するとき、操作者により指定された復号キーに従って暗号データが復号化され、その復号データつまり非暗号データをアクセス対象とするような非暗号モードが設定される。

【0026】このように、電波環境の変化に応じて暗号化/復号化が行われ、また、携帯端末上のデータをオフィスに設置されたネットワーク上で共有資源としてPCにより共有化/非共有化する場合でも暗号化/復号化が行われる。これにより、携帯端末の利便性をさらに向上させることができる。

【0027】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を説明する。

【0028】ここでは、第1の実施形態としてオフィスと移動環境間で携帯端末を使用する場合、第2の実施形態としてネットワーク上で携帯端末を共有化/非共有化する場合、第3の実施形態として無線環境で携帯端末を使用する場合をそれぞれ想定したセキュリティシステムについて説明する。

【0029】(第1の実施形態)図1は本発明の第1の実施形態に係るシステムの全体構成を示すブロック図である。図1に示すように、オフィス10と移動環境12を想定する。

【0030】オフィス10では、通信機能を備えた携帯端末10-1a、…、10-1nが無線LAN基地局10-2aと無線LANハブ10-2bからなる無線LAN10-2に通信により接続可能であり、さらにLAN10-3を介してPC(パーソナルコンピュータ)10-4a、…、10-4nとサーバコンピュータ10-5にも接続可能である。

【0031】一方、移動環境12では、同じく通信機能を備えた携帯端末12-1a、…、12-1nが移動通信網基地局12-2を介して移動通信網12-3に通信により接続可能である。LAN10-3と移動通信網12-3は交換機11により接続されている。

【0032】オフィス10での携帯端末10-1a、…、10-1nと移動環境12での携帯端末12-1a、…、12-1nは同一のものである。すなわち、オフィス10と移動環境12との間を移動しながら携帯端末10-1a、…、10-1nを使用する。以降の説明では携帯端末10-1aを用いて説明する。

【0033】まず、携帯端末10-1aの構成を図2を用いて説明する。

【0034】図2は第1の実施形態における携帯端末10-1aの構成を示すブロック図である。図2に示すように、携帯端末10-1aは、CPU21、メモリ22、2次記憶装置23、LCD(Liquid Crystal Display)やCRT(Cathode Ray Tube)などの画面表示装置24、キーボードやマウスなどの入力装置25、無線LAN10-2や移動通信網12-3との通信を制御する通信制御装置26から構成される。

【0035】メモリ22上には、画面表示を制御する画面制御プログラム22-1、2次記憶装置23上の非暗号データを暗号化するための暗号キーを暗号キーレジスタに設定したり、2次記憶装置23上の暗号データを復号化するための復号キーを復号キーレジスタに設定するキー設定プログラム22-2、2次記憶装置23上のデータをアクセスする暗復号化プログラム22-3、暗復号化プログラム22-3が2次記憶装置23上のデータをアクセスするときに使用するデータバッファ22-4が置かれている。

【0036】2次記憶装置23は、例えばPCカードのような超小型の記憶装置あるいは磁気ディスクやフラッ

シメメモリなどの不揮発性メモリからなる。この2次記憶装置23上には、選択回路23-1、モードレジスタ23-1a、暗号キーレジスタ23-2、暗号化書込回路23-3、暗号データ記憶部23-4、復号キーレジスタ23-5、復号化読出回路23-6、書込回路23-7、非暗号データ記憶部23-8、読出回路23-9が置かれている。

【0037】選択回路23-1は、キー設定プログラム22-2からのキー設定要求タイプ（暗号キーか復号キーのどちらかを設定）と暗復号化プログラム22-3からのアクセス要求タイプ（非暗号データや暗号データの読取りと書込み）を選択する。モードレジスタ23-1aは、選択回路23-1内にあって移動環境12で非暗号データをアクセスするのか暗号データをアクセスするのかのモードを保持する。

【0038】暗号キーレジスタ23-2は、暗号キーを保持する。暗号化書込回路23-3は、暗復号化プログラム22-3からのデータを暗号化して暗号データ記憶部23-4に書込む。暗号データ記憶部23-4は、暗号化されたデータを記憶する。復号キーレジスタ23-5は、復号キーを保持する。復号化読出回路23-6は、暗号データ記憶部23-4のデータを復号化して読出す。書込回路23-7は、非暗号データを非暗号データ記憶部23-8に書込む。非暗号データ記憶部23-8は、非暗号データを記憶する。読出回路23-9は、非暗号データ記憶部23-8のデータを読出す。

【0039】次に、携帯端末10-1aの操作画面を図3を用いて説明する。

【0040】図3は第1の実施形態における携帯端末10-1aの操作画面を示す図である。図3に示すように、携帯端末10-1aの操作画面3は、操作者がキー設定プログラム22-2を用いて暗号キーを暗号キーレジスタ23-2に設定するための画面31、暗号データを復号データに戻すときに使用する復号キーをキー設定プログラムにより復号キーレジスタ23-5に設定するための画面32、操作者が実際に2次記憶装置23上の非暗号データまたは暗号データをアクセスするための画面33の3つから構成される。

【0041】画面31では、操作者はパスワード31-1の入力により正当な操作者であることが認証された後、暗号キー31-2に暗号キーを指定し、暗号キー設定アイコン31-3をクリックする。これにより、キー設定プログラム22-2は暗号キー31-2に指定された暗号キーを2次記憶装置23上の暗号キーレジスタ23-2に格納する。

【0042】画面32では、操作者はパスワード32-1の入力により正当な操作者であることが認証された後、復号キー32-2に復号キーを指定し、復号キー設定アイコン32-3をクリックする。これにより、キー設定プログラム22-2は復号キー32-2に指定され

た復号キーを2次記憶装置23上の復号キーレジスタ23-5に格納する。

【0043】画面33では、操作者がオフィス10にいる場合と移動環境12にいる場合とで異なる。すなわち、操作者がオフィス10にいて移動環境12に移動するときに選択する暗号化アイコン33-1と、移動環境12からオフィス10に戻ったときに選択する復号化アイコン33-3と、暗号化または復号化の状況（例えばデータが現在何%暗号化または復号化されているのかを示す完了度合など）を示す状況表示画面33-2から構成される。

【0044】ここで、暗号化の場合には、暗号化アイコン33-1の選択により、暗復号化プログラム22-3は以下のような一連の暗号化コピー処理を実行することになる。

【0045】すなわち、読出回路23-9によりメモリ22上のデータバッファ22-4に読み出した非暗号データ記憶部23-8のデータを暗号化書込回路23-3により暗号キーレジスタ23-2内の暗号キーを用いて暗号化し、その暗号化されたデータを暗号化書込回路23-3により暗号データ記憶部23-4に書込む。また、復号化の場合には、復号化アイコン33-3の選択により、暗復号化プログラム22-3は以下のような一連の復号化コピー処理を実行することになる。

【0046】すなわち、暗号データ記憶部23-4のデータを復号化読出回路23-6により読み出して復号キーレジスタ23-5内の復号キーを用いて復号化し、その復号化されたデータ（つまり非暗号データ）を書込回路23-7により非暗号データ記憶部23-8に書込む。

【0047】なお、図3の例では、暗号化の設定画面と復号化の設定画面の一体化された構成を示したが、例えば暗号化時には画面31と、暗号化アイコン33-1および状況表示画面33-2を表示し、暗号化時には画面32と、復号化アイコン33-3および状況表示画面33-2を表示するようにしても良い。

【0048】次に、図1～図3を前提にしてオフィス10と移動環境12との間の移動時におけるデータの暗号化と復号化の処理の流れを説明する。

【0049】まず、オフィス10から移動環境12に移動するときの操作及び処理について図4および図5を用いて説明する。

【0050】図4および図5は第1の実施形態における暗号化処理の動作を説明するためのフローチャートである。オフィス10から移動環境12に移動するとき、操作者が操作画面31でパスワード31-1を入力し、正当な操作者であることが認証された後、暗号キー31-2を入力して暗号キー設定アイコン31-3をクリックする（ステップA11）。これにより、キー設定プログラム22-2は2次記憶装置23上の暗号キーレジスタ



23-2に暗号キー31-2を設定する(ステップA12)。

【0051】操作者が暗号化アイコン33-1をクリックすると(ステップA13)、暗復号化プログラム22-3は選択回路23-1に対して非暗号データ記憶部23-8上のデータをメモリ22上のデータバッファ22-4に読み出すことを指令する(ステップA14)。

【0052】この暗復号化プログラム22-3による指令を受けた選択回路23-1は、読出回路23-9により非暗号データ記憶部23-8から非暗号データを読み出し、その非暗号データをメモリ22上のデータバッファ22-4に格納する(ステップA15)。

【0053】次に、暗復号化プログラム22-3は、データバッファ22-4上の非暗号データを選択回路23-1に暗号化して暗号データ記憶部23-4に格納することを指令する(ステップA16)。

【0054】この暗復号化プログラム22-3による指令を受けた選択回路23-1は、暗号化書込回路23-3によりデータバッファ22-4上の非暗号データを暗号キーレジスタ23-2内の暗号キーを用いて暗号化し、これを暗号データ記憶部23-4に書込む(ステップA17)。

【0055】このとき、暗復号化プログラム22-3は暗号化処理の完了度合(暗号化が何%完了したか)などの状況を画面33の状況表示画面33-2に表示する(ステップA18)。

【0056】以上の読出処理と暗号化書込処理を非暗号データ記憶部23-8上のデータがなくなるまで繰り返す(ステップA19)。非暗号データ記憶部23-8上のデータがなくなると(ステップA19のNo)、暗復号化プログラム22-3は選択回路23-1内のモードレジスタ23-1aを以降の2次記憶装置23へのアクセスが暗号データ記憶部23-4に対して行われるように暗号モードに設定し(ステップA20)、暗号化処理完了のメッセージを状況表示画面33-2に表示する(ステップA21)。

【0057】次に、移動環境12からオフィス10に移動するときの操作及び処理について図6および図7を用いて説明する。

【0058】図6および図7は第1の実施形態における復号化処理の動作を説明するためのフローチャートである。移動環境12からオフィス10に移動するとき、操作者が操作画面32でパスワード32-1を入力し、正当な操作者であることが認証された後、復号キー32-2を入力して復号キー設定アイコン32-3をクリックする(ステップB11)。これにより、キー設定プログラム22-2は2次記憶装置23上の復号キーレジスタ23-5に復号キー32-2を設定する(ステップB12)。

【0059】操作者が復号化アイコン33-3をクリッ

クすると(ステップB13)、暗復号化プログラム22-3は選択回路23-1に対して暗号データ記憶部23-4上のデータをメモリ22上のデータバッファ22-4に読み出すことを指令する(ステップB14)。

【0060】この暗復号化プログラム22-3による指令を受けた選択回路23-1は復号化読出回路23-6により暗号データ記憶部23-4から暗号データを読み出して復号キーレジスタ23-5内の復号キーを用いて復号化し、その復号化されたデータをメモリ22上のデータバッファ22-4に格納する(ステップB15)。

【0061】次に、暗復号化プログラム22-3はデータバッファ22-4上の復号化されたデータを選択回路23-1に対して非暗号データ記憶部23-8に格納することを指令する(ステップB16)。

【0062】この暗復号化プログラム22-3による指令を受けた選択回路23-1は、書込回路23-7により非暗号データ記憶部23-8にデータバッファ22-4上の非暗号データを書込む(ステップB17)。

【0063】このとき、暗復号化プログラム22-3は復号化処理の完了度合(復号化が何%完了したか)などの状況を画面33の状況表示画面33-2に表示する(ステップB18)。

【0064】以上の暗号化読出処理と書込処理を暗号データ記憶部23-4上のデータがなくなるまで繰り返す(ステップB19)。暗号データ記憶部23-4上のデータがなくなると(ステップB19のNo)、暗復号化プログラム22-3は選択回路23-1内のモードレジスタ23-1aを以降の2次記憶装置23へのアクセスが非暗号データ記憶部23-8に対して行われるように非暗号モードに設定し(ステップB20)、復号化処理完了のメッセージを状況表示画面33-2に表示する(ステップB21)。

【0065】このように、第1の実施形態にあっては、オフィスから移動環境に移動するときには、操作者が指定した暗号キーに従って携帯端末上のデータを暗号化して持ち歩くことができる。つまり、操作者のみが知る暗号キーを用いて暗号化できる。これにより、移動環境において、盗難や置き忘れなどによってデータが漏洩してしまうのを防ぐことができる。一方、移動環境からオフィスに戻るときには、操作者が指定した暗号キーに従って、その暗号データを復号化して元に戻すことができる。これにより、オフィス内では、常に誰もがデータを確認することができる。

【0066】(第2の実施形態) 上述した第1の実施形態では、操作者がプログラムに指示して暗号化あるいは復号化を行っているが、第2の実施形態では、携帯端末のデータをPCのデータとしてLANや無線LANを介して共有すること(これをネットワーク共有化と呼ぶ)を復号化実行のトリガーとし、逆に非共有にすること(これをネットワーク非共有化と呼ぶ)を暗号化実行の

トリガーとすることで、前述の操作者の指示の代わりとする。

【0067】すなわち、通常、オフィスでは、携帯端末を使用せずに高性能で使い易いPCを使用するが、この場合に必要なのは携帯端末上のデータをPCが処理できるようにネットワーク共有化することである。第2の実施形態では、このことに着目し、オフィスでPCが携帯端末上のデータをネットワーク共有化し処理している状況ではデータは復号化し、PCによりネットワーク非共有化されたとき移動環境に携帯端末が移動したものとみなし、それをトリガーとして携帯端末上のデータを暗号化する。

【0068】以下、図面を参照して本発明の第2の実施形態を説明する。

【0069】図8は本発明の第2の実施形態に係るシステムの全体構成を示すブロック図である。図8に示すように、オフィス10aと移動環境12aを想定する。

【0070】オフィス10aでは、通信機能を備えた携帯端末10a-1a、…、10a-1nが無線LAN基地局10a-2aと無線LANハブ10a-2bからなる無線LAN10a-2と通信により接続可能であり、さらにLAN10a-3を介してPC（パーソナルコンピュータ）10a-41、…、10a-4nとサーバコンピュータ10a-5にも接続可能である。

【0071】一方、移動環境12aでは、同じく通信機能を備えた携帯端末12a-1a、…、12a-1nが移動通信網基地局12a-2を介して移動通信網12a-3に通信により接続可能である。LAN10a-3と移動通信網12a-3は交換機11aにより接続されている。

【0072】オフィス10aでの携帯端末10a-1a、…、10a-1nと移動環境12aでの携帯端末12a-1a、…、12a-1nは同一のものである。すなわち、オフィス10aと移動環境12aとの間を移動しながら携帯端末10a-1a、…、10a-1nを使用する。

【0073】また、携帯端末10a-1a、…、10a-1nのデータはPC10a-4a、…、10a-4nによってネットワーク共有化され、ネットワーク共有化時には携帯端末10a-1a、…、10a-1nに内蔵されている2次記憶装置はPC10a-4a、…、10a-4nの第2の2次記憶装置として機能し、携帯端末10a-1a…10a-1nの2次記憶装置上のデータはPC10a-4a上の別の2次記憶装置上のデータとして共有される。PC10a-4a…、10a-4nによってネットワーク非共有化されると、携帯端末10a-1a、…、10a-1nの2次記憶装置としてのみ機能する。

【0074】さらに1台のPCが複数台の携帯端末をネットワーク共有化できるが、以降ではPC10a-4a

が携帯端末10a-1a上のデータをネットワーク共有化することを前提として説明する。

【0075】まず、PC10a-4aの構成を図9を用いて説明する。

【0076】図9は第2の実施形態におけるPC10a-4aの構成を示すブロック図である。図9に示すように、PC10a-4aは、CPU21a、メモリ22a、2次記憶装置23a、LCD（Liquid Crystal Display）やCRT（Cathode RayTube）などの画面表示装置24a、キーボードやマウスなどの入力装置25a、LANとの通信を制御する通信制御装置26a、ネットワーク共有化された2次記憶装置27aから構成される。この2次記憶装置27aは、ネットワーク共有化された場合に使用される仮想的な記憶装置である。

【0077】メモリ22a上には、画面表示を制御する画面制御プログラム22a-1、携帯端末10a-1aの2次記憶装置上のデータをネットワーク共有化／非共有化するネットワーク共有化プログラム22a-2が置かれている。

【0078】次に、PC10a-4aの操作画面を図10を用いて説明する。

【0079】図10は第2の実施形態における携帯端末10-1aの操作画面を示す図である。図10に示すように、PC10a-4aの操作画面3aは、ネットワーク共有化を設定するための画面3a-1、ネットワーク非共有化を設定するための画面3a-2、現在共有化されている端末名を表示するための画面3a-3から構成される。

【0080】画面3a-1では、ネットワーク共有化するデータを持つ携帯端末10a-1aの名前3a-1a、携帯端末10a-1aの操作者のユーザ識別子3a-1b、同操作者のパスワード3a-1c、携帯端末10a-1aの復号化キー3a-1aを入力する。

【0081】画面3a-2では、ネットワーク非共有化するデータを持つ携帯端末10a-1aの名前3a-2a、携帯端末10a-1aの操作者のユーザ識別子3a-2b、同操作者のパスワード3a-2c、携帯端末10a-1aの復号化キー3a-2dを入力する。

【0082】画面3a-3では、現在ネットワーク共有化している携帯端末10a-1aの名前3a-3aを表示する。

【0083】次に、携帯端末10a-1aの構成を図11を用いて説明する。

【0084】図11は第2の実施形態における携帯端末10a-1aの構成を示すブロック図である。図11に示すように、携帯端末10a-1aは、CPU41a、メモリ42a、2次記憶装置43a、LCD（Liquid Crystal Display）やCRT（Cathode Ray Tube）などの画面表示装置44a、キーボードやマウスなどの入力装置45a、無線LAN10a-2や移動通信網12a-

3との通信を制御する通信制御装置46aから構成される。

【0085】メモリ42a上には、画面表示を制御する画面制御プログラム42a-1、2次記憶装置43a上の非暗号データを暗号化するための暗号キーを暗号キーレジスタに設定したり、2次記憶装置43a上の暗号データを復号化するための復号キーを復号キーレジスタに設定するキー設定プログラム42a-2、2次記憶装置43a上のデータを暗号化したり復号化するためにアクセスする暗号化プログラム42a-3、暗号化プログラム42a-3が2次記憶装置43a上のデータをアクセスするときに使用するデータバッファ42a-4が置かれている。さらに、ここでは、PC10a-4aによって携帯端末10a-1aの2次記憶装置43aがネットワーク共有化されたとき、あるいは、ネットワーク非共有化されたときにPC10a-4aが携帯端末10a-1aに送信する通知メッセージを検出するネットワーク共有化検出プログラム42a-5が置かれている。2次記憶装置43aは、例えばPCカードのような超小型の記憶装置あるいは磁気ディスクやフラッシュメモリなどの不揮発性メモリからなる。この2次記憶装置43a上には、選択回路43a-1、モードレジスタ43a-1a、暗号キーレジスタ43a-2、暗号化書込回路43a-3、暗号データ記憶部43a-4、復号キーレジスタ43a-5、復号化読出回路43a-6、書込回路43a-7、非暗号データ記憶部43a-8、読出回路43a-9が置かれている。

【0086】選択回路43a-1は、キー設定プログラム42a-2からのキー設定要求タイプ（暗号キーか復号キーのどちらかを設定）と暗号化プログラム42a-3からのアクセス要求タイプ（非暗号データや暗号データの読取りと書込み）を選択する。モードレジスタ43a-1aは、選択回路43a-1内にあって移動環境12aで非暗号データをアクセスするのか暗号データをアクセスするのかのモードを保持する。

【0087】暗号キーレジスタ43a-2は、暗号キーを保持する。暗号化書込回路43a-3は、暗号化プログラム42a-3からのデータを暗号化して暗号データ記憶部43a-4に書込む。暗号データ記憶部43a-4は、暗号化されたデータを記憶する。復号キーレジスタ43a-5は、復号キーを保持する。復号化読出回路43a-6は、暗号データ記憶部43a-4のデータを復号化して読出す。書込回路43a-7は、非暗号データを非暗号データ記憶部43a-8に書込む。非暗号データ記憶部43a-8は、非暗号データを記憶する。読出回路43a-9は、非暗号データ記憶部43a-8のデータを読出す。

【0088】次に、携帯端末10a-1aの操作画面を図12を用いて説明する。

【0089】図12は第2の実施形態における携帯端末

10a-1aの操作画面を示す図である。図12に示すように、携帯端末10a-1aの操作画面5aは、ネットワーク共有化時の2次記憶装置43a上のデータの復号化/暗号化の状況を表示するための画面51aから構成される。

【0090】画面51aでは、携帯端末10a-1aの2次記憶装置43a上のデータがPC10a-4aによってネットワーク非共有化された場合とネットワーク共有化された場合とで異なる。すなわち、ネットワーク非共有時は、暗号化コピー処理を実行する暗号化プログラム42a-3の実行状況と暗号化完了時のネットワーク共有化PC10a-4aの名前表示がなされる。逆に、ネットワーク共有化時は、復号化コピー処理を実行する暗号化プログラム42a-3の実行状況表示と復号化完了時のネットワーク共有化PC10a-4aの名前の消去がなされる。

【0091】次に、図8～図11を前提にしてオフィス10aと移動環境12aとの間の移動時におけるデータの暗号化と復号化の処理の流れを説明する。

【0092】まず、オフィス10aから移動環境12aに移動するときの操作及び処理について図6を用いて説明する。

【0093】図13および図14は第2の実施形態におけるネットワーク非共有化処理（暗号化処理）の動作を説明するためのフローチャートである。オフィス10aから移動環境12aに移動するとき、PC10a-4aから携帯端末10a-1aの2次記憶装置43a上のデータをネットワーク非共有化とする。このため、PC10a-4aの操作画面3a-2において、操作者がネットワーク非共有化の対象となる携帯端末10a-1aの名前3a-2a、携帯端末10a-1aの操作者のユーザ識別子3a-2bとパスワード3a-2c、携帯端末のデータの暗号キー3a-2dを入力する（ステップC11）。

【0094】この入力に従い、PC10a-4aのネットワーク共有化プログラム22a-2はネットワーク非共有化実行の通知メッセージをユーザ識別子3a-2bとパスワード3a-2c、暗号キー3a-2dと共に名前3a-2aに指定された携帯端末10a-1aに送信する（ステップC12）。

【0095】この通知メッセージを受信した携帯端末10a-1aのネットワーク共有化検出プログラム42a-5は、受信したユーザ識別子3a-2bとパスワード3a-2cが携帯端末10a-1aの操作者のものと一致するか否かを確認する（ステップC13）。その結果、正当な操作者であることを認証すると（ステップCのYes）、キー設定プログラム42a-2に制御を移し、キー設定プログラム42a-2は2次記憶装置43a上の暗号キーレジスタ43a-2に通知メッセージ内の暗号キー3a-2dを設定する（ステップC14）。

【0096】ここで、暗復号化プログラム42a-3は選択回路43a-1に対して非暗号データ記憶部43a-8上のデータをメモリ42a上のデータバッファ42a-4に読み出すことを指令する(ステップC15)。

【0097】この暗復号化プログラム42a-3による指令を受けた選択回路43a-1は、読出回路43a-9により非暗号データ記憶部43a-8から非暗号データを読み出し、その非暗号データをメモリ42a上のデータバッファ42a-4に格納する(ステップC16)。

【0098】次に、暗復号化プログラム42a-3は、データバッファ42a-4上の非暗号データを選択回路43a-1に暗号化して暗号データ記憶部43a-4に格納することを指令する(ステップC17)。

【0099】この暗復号化プログラム42a-3による指令を受けた選択回路43a-1は、暗号化書込回路43a-3により暗号データ記憶部43a-4にデータバッファ42a-4上の非暗号データを暗号キーレジスタ43a-2内の暗号キーを用いて暗号化し、これを暗号データ記憶部43a-4に書込む(ステップC18)。

【0100】このとき、暗復号化プログラム42a-3は暗号化処理の完了度合(暗号化が何%完了したか)などの状況を画面53aの状況表示画面53a-2に表示する(ステップC19)。

【0101】以上の読出処理と暗号化書込処理を非暗号データ記憶部43a-8上のデータがなくなるまで繰り返す(ステップC20)。非暗号データ記憶部43a-8上のデータがなくなると(ステップC20のNo)、暗復号化プログラム42a-3は選択回路43a-1内のモードレジスタ43a-1aを以降の2次記憶装置へのアクセスが暗号データ記憶部43a-8に対して行われるように暗号モードに設定する(ステップC21)。

【0102】また、暗復号化プログラム42a-3は暗号化処理完了のメッセージをPC10a-4aに通知すると共に、その暗号化処理完了のメッセージを状況表示画面51aに表示して、これまで表示されていたネットワーク共有化PC10a-4aの名前を消去する(ステップC22)。

【0103】一方、上記ステップC13において、ネットワーク共有化検出プログラム42a-5が不当な操作者であることを検出した場合には(ステップC13のNo)、エラーメッセージをPC10a-4aに返信すると共に、そのエラーメッセージを状況表示画面に表示して、直ちにデータの暗号化を中止する(ステップC23)。

【0104】次に、移動環境12aからオフィス10aに移動するときの操作及び処理について図15および図16を用いて説明する。

【0105】図15および図16は第2の実施形態におけるネットワーク共有化処理(復号化処理)の動作を説

明するためのフローチャートである。移動環境12aからオフィス10aに移動するとき、PC10a-4aから携帯端末10a-1aの2次記憶装置43a上のデータをネットワーク共有化とする。このため、PC10a-4aの操作画面3a-1において、操作者がネットワーク共有化の対象となる携帯端末10a-1aの名前3a-1a、携帯端末10a-1aの操作者のユーザ識別子3a-1bとパスワード3a-1c、携帯端末のデータの復号キー3a-1dを入力する(ステップD11)。

【0106】この入力に従い、PC10a-4aのネットワーク共有化プログラム22a-2はネットワーク共有化実行の通知メッセージをユーザ識別子3a-1bとパスワード3a-1c、復号キー3a-1dと共に名前3a-1aに指定された携帯端末10a-1aに送信する(ステップD12)。

【0107】この通知メッセージを受信した携帯端末10a-1aのネットワーク共有化検出プログラム42a-5は、受信したユーザ識別子3a-1bとパスワード3a-1cが携帯端末10a-1aの操作者のものと一致するか否かを検査する(ステップD13)。その結果、正当な操作者であることを認証すると(ステップD13のYes)、キー設定プログラム42a-2に制御を移し、キー設定プログラム42a-2は2次記憶装置43a上の復号キーレジスタ43a-5に通知メッセージ内の復号キー3a-1dを設定する(ステップD14)。

【0108】ここで、暗復号化プログラム42a-3は選択回路43a-1に対して暗号データ記憶部43a-4上のデータをメモリ42a上のデータバッファ42a-4に読み出すことを指令する(ステップD15)。

【0109】この暗復号化プログラム42a-3による指令を受けた選択回路43a-1は、復号化読出回路43a-6により暗号データ記憶部43a-4から暗号データを読み出して復号キーレジスタ43a-5内の復号キーを用いて復号化し、その復号化されたデータをメモリ42a上のデータバッファ42a-4に格納する(ステップD16)。

【0110】次に、暗復号化プログラム42a-3は、データバッファ42a-4上の復号化されたデータを選択回路43a-1に対して非暗号データ記憶部43a-8に格納することを指令する(ステップD17)。

【0111】この暗復号化プログラム42a-3による指令を受けた選択回路43a-1は、書込回路43a-7により非暗号データ記憶部43a-8にデータバッファ42a-4上の非暗号データを書込む(ステップD18)。

【0112】このとき、暗復号化プログラム42a-3は復号化処理の完了度合(復号化が何%完了したか)などの状況を画面53aの状況表示画面53a-2に表示

10

20

30

40

50

する(ステップD19)。

【0113】以上の暗号化読出処理と書込処理を暗号データ記憶部43a-4上のデータがなくなるまで繰り返す(ステップD20)。暗号データ記憶部43a-4上のデータがなくなると(ステップD20のNo)、暗号化プログラム42a-3は選択回路43a-1内のモードレジスタ43a-1aを以降の2次記憶装置へのアクセスが非暗号データ記憶部43a-8に対して行われるように非暗号モードに設定する(ステップD21)。

【0114】また、暗号化プログラム42a-3は復号化処理完了のメッセージをPC10a-4aに通知すると共に、その復号化処理完了のメッセージを状況表示画面53a-2に表示して、ネットワーク共有化PC10a-4aの名前を表示する(ステップD22)。

【0115】一方、上記ステップD13において、ネットワーク共有化検出プログラム42a-5が不当な操作者であることを検出すると(ステップD13のNo)、エラーメッセージをPC10a-4aに返信すると共に、そのエラーメッセージを状況表示画面に表示して、直ちにデータの復号化を中止する(ステップD23)。このように、第2の実施形態にあつては、携帯端末上のデータをオフィスに設置されたネットワーク上で共有資源としてPCにより共有化(PCに論理的に取り付けることと同義)している間は暗号データが復号化される。一方、非共有化(PCから論理的に取り外すことと同義)したときには、データが暗号化されるといった柔軟でかつ安全性の高い携帯端末の利用を実現できる。これにより、移動環境に限らずオフィス内での盗難や置き忘れ時にもデータ保護ができる携帯端末を提供できる。

【0116】(第3の実施形態) 上述した第1の実施形態では、操作者がプログラムに指示して暗号化あるいは復号化を行っているが、第3の実施形態では、携帯端末が電波の強度と種別を検出することにより、操作者が自分の存在する環境を認識して暗号化か復号化かを指定するのではなく、その環境で最強の電波がオフィス内で使用されている無線LANなのかあるいは移動通信環境で使用されている移動通信網なのかを自動的に判断する。そして、最強の電波が無線LANの規格のものであれば携帯端末のデータを復号化し、移動通信網の規格のものであれば暗号化することにより、利便性の高い携帯端末を提供する。

【0117】以下、図面を参照して本発明の第3の実施形態を説明する。

【0118】図17は本発明の第3の実施形態に係るシステムの全体構成を示すブロック図である。図17に示すように、オフィス10bと移動環境12bを想定する。

【0119】オフィス10bでは、通信機能を備えた携帯端末10b-1a、…、10b-1nが無線LAN基地局10b-2aと無線LANハブ10b-2bからな

る無線LAN10b-2と通信により接続可能であり、さらにLAN10b-3を介してPC(パーソナルコンピュータ)10b-4a、…、10b-4nとサーバコンピュータ10b-5にも接続可能である。

【0120】一方、移動環境12bでは、同じく通信機能を備えた携帯端末12b-1a、…、12b-1nが移動通信網基地局12b-2を介して移動通信網12b-3に通信により接続可能である。LAN10b-3と移動通信網12b-3は交換機11bにより接続されている。

【0121】オフィス10bでの携帯端末10b-1a、…、10b-1nと移動環境12bでの携帯端末12b-1a、…、12b-1nは同一のものである。すなわち、オフィス10bと移動環境12bとの間を移動しながら携帯端末10b-1a、…、10b-1nを使用する。以降の説明では携帯端末10b-1aを用いて説明する。

【0122】まず、携帯端末10b-1aの構成を図18を用いて説明する。

【0123】図18は第3の実施形態における携帯端末10b-1aの構成を示すブロック図である。図18に示すように、携帯端末10b-1aは、CPU21b、メモリ22b-2次記憶装置23b、LCD(Liquid Crystal Display)やCRT(Cathode Ray Tube)などの画面表示装置24b、キーボードやマウスなどの入力装置25b、無線LAN10b-2や移動通信網12b-3との通信を制御する通信制御装置26b、無線LAN10b-2や移動通信網12b-3の電波の強度や種別を検出する電波検出装置27bから構成される。

【0124】メモリ22b上には、画面表示を制御する画面制御プログラム22b-1、2次記憶装置23b上の非暗号データを暗号化するための暗号キーを暗号キーレジスタに設定したり、2次記憶装置23b上の暗号データを復号化するための復号キーを復号キーレジスタに設定するキー設定プログラム22b-2、2次記憶装置23b上の暗号データか非暗号データのどちらをアクセスするのかの設定を行うモード設定プログラム22b-3が置かれている。

【0125】2次記憶装置23bは、例えばPCカードのような超小型の記憶装置あるいは磁気ディスクやフラッシュメモリなどの不揮発性メモリからなる。この2次記憶装置23b上には、選択回路23b-1、モードレジスタ23b-1a、暗号キーレジスタ23b-2、暗号化書込回路23b-3、暗号データ記憶部23b-4、復号キーレジスタ23b-5、復号化読出回路23b-6、書込回路23b-7、非暗号データ記憶部23b-8、読出回路23b-9が置かれている。

【0126】選択回路23b-1は、キー設定プログラム22b-2からのキー設定要求タイプ(暗号キーか復号キーのどちらかを設定)と暗号化プログラム22b-3

10

20

30

40

50

からのアクセス要求タイプ（非暗号データや暗号データの読取りと書き込み）を選択する。モードレジスタ23b-1aは、選択回路23b-1内にあって移動環境12bで非暗号データをアクセスするのか暗号データをアクセスするのかのモードを保持する。

【0127】暗号キーレジスタ23b-2は、暗号キーを保持する。暗号化書込回路23b-3は、暗号化プログラム22-3からのデータを暗号化して暗号データ記憶部23b-4に書込む。暗号データ記憶部23b-4は、暗号化されたデータを記憶する。復号キーレジスタ23b-5は、復号キーを保持する。復号化読出回路23b-6は、暗号データ記憶部23b-4のデータを復号化して読出す。書込回路23b-7は、非暗号データを非暗号データ記憶部23b-8に書込む。非暗号データ記憶部23b-8は、非暗号データを記憶する。読出回路23b-9は、非暗号データ記憶部23b-8のデータを読出す。

【0128】次に、携帯端末10b-1aの操作画面を図19を用いて説明する。

【0129】図19は第3の実施形態における携帯端末10b-1aの操作画面を示す図である。図19に示すように、携帯端末10b-1aの操作画面3bは、操作者がキー設定プログラム22b-2を用いて暗号キーを暗号キーレジスタ23b-2に設定するための画面31b、暗号データを復号データに戻すときに使用する復号キーをキー設定プログラムにより復号キーレジスタ23b-5に設定するための画面32b、操作者が実際に2次記憶装置23b上の非暗号データまたは暗号データをアクセスするための画面33bの3つから構成される。

【0130】電波検出プログラム22b-4が電波検出装置27bを通じて検出した最強の電波が移動環境12bで利用されている移動通信網の規格の電波であれば、画面31bを表示して操作者に暗号手続きを促す。これに対し、操作者はパスワード31b-1を入力して正当な操作者であることが認証された後、暗号キー31b-2に暗号キーを指定して暗号キー設定アイコン31b-3をクリックする。これにより、キー設定プログラム22b-2は暗号キー31b-2に指定された暗号キーを2次記憶装置23b上の暗号キーレジスタ23b-2に設定する。

【0131】また、電波検出プログラム22b-4の検出した電波が無線LANの電波であれば、画面32bを表示して操作者に復号化の手続きを促す。これに対し、操作者はパスワード32b-1を入力して正当な操作者であることが認証された後、復号キー32b-2に復号キーを指定し、復号キー設定アイコン32b-3をクリックする。これにより、キー設定プログラム22b-2は復号キー32b-2に指定された復号キーを2次記憶装置23b上の復号キーレジスタ23b-5に設定する。

【0132】画面33bは、暗号化プログラム22b-3の実行の状況表示画面であり、暗号化または復号化の状況（例えばデータが現在何%暗号化または復号化されているのかを示す完了度合など）を示す。

【0133】次に、図17～図19を前提にしてオフィス10bと移動環境12bとの間の移動時におけるデータの暗号化と復号化の処理の流れを説明する。

【0134】まず、電波検出とその種別分析に基づく暗号化あるいは復号化処理の実行について図20を用いて説明する。

【0135】図20は第3の実施形態における電波種別に応じた暗号化／復号化の判断処理の動作を説明するためのフローチャートである。携帯端末10b-1aの存在する環境がオフィス10bから移動環境12bかを電波検出プログラム22b-4が電波検出装置27bを利用して検出分析する（ステップE11）。その際に、前回の検出時の電波種別と同じか否かを検査し（ステップE12）、異なっている場合には（ステップE12のNo）。電波がどの規格かを検査する（ステップE13）。

【0136】ここで、移動環境12bにおける移動通信網12b-3の規格の電波であれば、後述する図21および図22に示す暗号化処理のサブルーチン呼び出す（ステップE14）。一方、オフィス10bにおける無線LAN10b-2の電波であれば、後述する図23および図24に示す復号化処理のサブルーチン呼び出す（ステップE15）。制御が戻されたら、あるいはステップE12で前回と同一電波であれば、ここでの処理を終了する。

【0137】なお、移動通信網の電波としては、携帯電話で1.5GHz、PHSで1.9GHzが使用されている。これに対し、無線LANの電波としては、2.4GHzと1.9GHzが使用されている。

【0138】次に、暗号化処理について図21および図22を用いて説明する。

【0139】図21および図22は第3の実施形態における暗号化処理の動作を説明するためのフローチャートである。受信電波の種類が移動環境12bにおける移動通信網12b-3の規格の電波であったとき、操作者が操作画面31bでパスワード31b-1を入力し、正当な操作者であることが認証された後、暗号キー31b-2を入力して暗号キー設定アイコン31b-3をクリックする（ステップF11）。これにより、キー設定プログラム22b-2は2次記憶装置23b上の暗号キーレジスタ23b-2に暗号キー31b-2を設定する（ステップF12）。操作者が暗号化アイコン33b-1をクリックすると（ステップF13）、暗号化プログラム22b-3は選択回路23b-1に対して非暗号データ記憶部23b-8上のデータをメモリ22b上のデータバッファ22b-4に読み出すことを指令する（ステッ

ブF14)。

【0140】この暗復号化プログラム22b-3による指令を受けた選択回路23b-1は読出回路23b-9により非暗号データ記憶部23b-8から非暗号データを読み出し、その非暗号データをメモリ22b上のデータバッファ22b-4に格納する(ステップF15)。

【0141】次に、暗復号化プログラム22b-3は、データバッファ22b-4上の非暗号データを選択回路23b-1に暗号化して暗号データ記憶部23b-4に格納することを指令する(ステップF16)。

【0142】この暗復号化プログラム22b-3による指令を受けた選択回路23b-1は、暗号化書込回路23b-3によりデータバッファ22b-4上の非暗号データを暗号キーレジスタ23b-2内の暗号キーを用いて暗号化し、これを暗号データ記憶部23b-4に書込む(ステップF17)。

【0143】このとき、暗復号化プログラム22b-3は暗号化処理の完了度合(暗号化が何%完了したか)などの状況を画面33の状況表示画面33b-2に表示する(ステップF18)。

【0144】以上の読出処理と暗号化書込処理を非暗号データ記憶部23b-8上のデータがなくなるまで繰り返す(ステップF19)。非暗号データ記憶部23b-8上のデータがなくなると(ステップF19のNo)、暗復号化プログラム22b-3は選択回路23b-1内のモードレジスタ23b-1aを以降の2次記憶装置23bへのアクセスが暗号データ記憶部23b-4に対して行われるように暗号モードに設定し(ステップF20)、暗号化処理完了のメッセージを状況表示画面33b-2に表示する(ステップF21)。

【0145】次に、復号化処理について図23および図24を用いて説明する。

【0146】図23および図24は第3の実施形態における復号化処理の動作を説明するためのフローチャートである。受信電波の種類がオフィス10bにおける無線LAN10b-2の電波であったとき、操作者が操作画面32bでパスワード32b-1を入力し、正当な操作者であることが認証された後、復号キー32b-2を入力して復号キー設定アイコン32b-3をクリックする(ステップG11)。これにより、キー設定プログラム22b-2は2次記憶装置23b上の復号キーレジスタ23b-5に復号キー32b-2を設定する(ステップG12)。

【0147】操作者が復号化アイコン33b-3をクリックすると(ステップG13)、暗復号化プログラム22b-3は選択回路23b-1に対して暗号データ記憶部23b-4上のデータをメモリ22b上のデータバッファ22b-4に読み出すことを指令する(ステップG14)。

【0148】この暗復号化プログラム22b-3による

指令を受けた選択回路23b-1は復号化読出回路23b-6により暗号データ記憶部23b-4から暗号データを読み出して復号キーレジスタ23b-5内の復号キーを用いて復号化し、その復号化されたデータをメモリ22b上のデータバッファ22b-4に格納する(ステップG15)。

【0149】次に、暗復号化プログラム22b-3は、データバッファ22b-4上の復号化されたデータを選択回路23b-1に対して非暗号データ記憶部23b-8に格納することを指令する(ステップG16)。

【0150】この暗復号化プログラム22b-3による指令を受けた選択回路23b-1は、書込回路23b-7により非暗号データ記憶部23b-8にデータバッファ22b-4上の非暗号データを書込む(ステップG17)。

【0151】このとき、復号化処理の完了度合(復号化が何%完了したか)などの状況を暗復号化プログラム22b-3は画面33bの状況表示画面33b-2に表示する(ステップG18)。

【0152】以上の暗号化読出処理と書込処理を暗号データ記憶部23b-4上のデータがなくなるまで繰り返す(ステップG19)。暗号データ記憶部23b-4上のデータがなくなると(ステップG19のNo)、暗復号化プログラム22b-3は選択回路23b-1内のモードレジスタ23b-1aを以降の2次記憶装置23bへのアクセスが非暗号データ記憶部23b-8に対して行われるように非暗号モードに設定し(ステップG20)、復号化処理完了のメッセージを状況表示画面33b-2に表示する(ステップG21)。

【0153】以上の暗号化処理と復号化処理は、電波環境の変化を常時チェックしておき、その変化を捕らえた時点でのみ実行される。例えば無線LANから移動通信網へ、あるいはこの逆といった場合で最初に電波の環境が切り換わった時点に実行される。このチェックは電波検出プログラム22b-4が行う。

【0154】このように、第3の実施形態にあつては、携帯端末の操作者が自分の存在する環境を意識することなく、電波環境の変化に応じて暗号化/復号化が自動的に行われる。これにより、操作者が自分の存在する環境では不適切であり、結果として誤った暗号化または復号化の処理を実行するといった操作ミスがなくすることができる。

【0155】なお、この第3の実施形態に上記第2の実施形態に適用することも可能である。この場合、携帯端末はオフィスまたは移動環境で使用されると共に、その携帯端末はネットワークに共有化または非共有化される。このような環境下において、移動環境に特有の電波が検出されたとき、あるいは、携帯端末をネットワークに非共有化するときには、操作者が指定した暗号キーに従って暗号化処理を行う。また、オフィスに特有の電波

が検出されたとき、あるいは、携帯端末をネットワークに共有化するときには、操作者が指定した復号キーに従って復号化処理を行う。

【0156】このように、電波環境の変化に応じて暗号化／復号化を行い、また、携帯端末上のデータをオフィスに設置されたネットワーク上で共有資源としてPCにより共有化／非共有化する場合に暗号化／復号化を行う構成とすることにより、利便性をさらに向上させることができる。

【0157】なお、上述した各実施形態において記載した手法は、コンピュータに実行させることのできるプログラムとして、例えば磁気ディスク（フロッピーディスク、ハードディスク等）、光ディスク（CD-ROM、DVD等）、半導体メモリなどの記憶媒体に書き込んで各種装置に適用したり、さらに通信媒体により伝送して各種装置に適用することも可能である。本システムを実現するコンピュータは、記録媒体に記録されたプログラムを読み込み、このプログラムによって動作が制御されることにより、上述した処理を実行する。

【0158】

【発明の効果】以上のように本発明によれば、携帯端末上のデータの暗号化／復号化を簡単に行うことができ、これにより、操作者に負担を掛けることなく、また、利便性に欠くことなくデータを保護することができる。

【0159】特に、携帯端末をオフィスから移動環境に移動させるとき、操作者により指定された暗号キーに従って携帯端末上の非暗号データを暗号化し、その暗号データをアクセス対象とするような暗号モードを設定し、携帯端末を移動環境からオフィスに移動させるとき、操作者により指定された復号キーに従って暗号データを復号化し、その復号データつまり非暗号データをアクセス対象とするような非暗号モードを設定するようにしたため、以下のような効果が得られる。

【0160】オフィスから移動環境に移動するときには、操作者が指定した暗号キーに従って携帯端末上のデータを暗号化して持ち歩くことができる。これにより、移動環境において、盗難や置き忘れなどによってデータが漏洩してしまうのを防ぐことができる。一方、移動環境からオフィスに戻るときには、操作者が指定した暗号キーに従って、その暗号データを復号化して元に戻すことができる。これにより、オフィス内では、常に誰もがデータを確認することができる。

【0161】また、携帯端末をネットワークに非共有化するとき、操作者により指定された暗号キーに従って携帯端末上の非暗号データを暗号化し、その暗号データをアクセス対象とするような暗号モードを設定し、携帯端末をネットワークに共有化するとき、携帯端末を移動環境からオフィスに移動させるとき、操作者により指定された復号キーに従って暗号データを復号化し、その復号データつまり非暗号データをアクセス対象とするような

非暗号モードを設定するようにしたため、以下のような効果が得られる。

【0162】携帯端末上のデータをオフィスに設置されたネットワーク上で共有資源としてPCにより共有化している間は暗号データが復号化される。一方、非共有化したときには、データが暗号化されるといった柔軟でかつ安全性の高い携帯端末の利用を実現できる。これにより、移動環境に限らずオフィス内での盗難や置き忘れ時にもデータ保護ができる携帯端末を提供できる。

10 【0163】また、携帯端末が受信する電波がオフィスに特有のものか移動環境に特有のものを検出し、移動環境に特有の電波であれば、操作者により指定された暗号キーに従って携帯端末上の非暗号データを暗号化し、その暗号データをアクセス対象とするような暗号モードを設定し、オフィスに特有の電波であれば、操作者により指定された復号キーに従って暗号データを復号化し、その復号データつまり非暗号データをアクセス対象とするような非暗号モードを設定するようにしたため、以下のような効果が得られる。

20 【0164】携帯端末の操作者が自分の存在する環境を意識することなく、電波環境の変化に応じて暗号化／復号化が自動的に行われる。これにより、操作者が自分の存在する環境では不適切であり、結果として誤った暗号化または復号化の処理を実行するといった操作ミスをなくすることができる。

【0165】また、移動環境に特有の電波を検出したとき、あるいは、携帯端末をネットワークに非共有化するとき、操作者により指定された暗号キーに従って携帯端末上の非暗号データを暗号化し、その暗号データをアクセス対象とするような暗号モードを設定し、オフィスに特有の電波を検出したとき、あるいは、携帯端末をネットワークに共有化するとき、操作者により指定された復号キーに従って暗号データを復号化し、その復号データつまり非暗号データをアクセス対象とするような非暗号モードを設定するようにしたため、以下のような効果が得られる。

【0166】電波環境の変化に応じて暗号化／復号化が行われ、また、携帯端末上のデータをオフィスに設置されたネットワーク上で共有資源としてPCにより共有化／非共有化する場合でも暗号化／復号化が行われる。これにより、携帯端末の利便性をさらに向上させることができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係るシステムの全体構成を示すブロック図。

【図2】第1の実施形態における携帯端末の構成を示すブロック図。

【図3】第1の実施形態における携帯端末の操作画面を示す図。

50 【図4】第1の実施形態における暗号化処理の動作を説



明するためのフローチャート。

【図 5】第 1 の実施形態における暗号化処理の動作を説明するためのフローチャート。

【図 6】第 1 の実施形態における復号化処理の動作を説明するためのフローチャート。

【図 7】第 1 の実施形態における復号化処理の動作を説明するためのフローチャート。

【図 8】本発明の第 2 の実施形態に係るシステムの全体構成を示すブロック図。

【図 9】第 2 の実施形態における PC の構成を示すブロック図。

【図 10】第 2 の実施形態における携帯端末の操作画面を示す図。

【図 11】第 2 の実施形態における携帯端末の構成を示すブロック図。

【図 12】第 2 の実施形態における携帯端末の操作画面を示す図。

【図 13】第 2 の実施形態におけるネットワーク非共有化処理（暗号化処理）の動作を説明するためのフローチャート。

【図 14】第 2 の実施形態におけるネットワーク非共有化処理（暗号化処理）の動作を説明するためのフローチャート。

【図 15】第 2 の実施形態におけるネットワーク共有化処理（復号化処理）の動作を説明するためのフローチャート。

【図 16】第 2 の実施形態におけるネットワーク共有化処理（復号化処理）の動作を説明するためのフローチャート。

【図 17】本発明の第 3 の実施形態に係るシステムの全体構成を示すブロック図。

【図 18】第 3 の実施形態における携帯端末の構成を示すブロック図。

【図 19】第 3 の実施形態における携帯端末の操作画面を示す図。

【図 20】第 3 の実施形態における電波種別に応じた暗

号化／復号化の判断処理の動作を説明するためのフローチャート。

【図 21】第 3 の実施形態における暗号化処理の動作を説明するためのフローチャート。

【図 22】第 3 の実施形態における暗号化処理の動作を説明するためのフローチャート。

【図 23】第 3 の実施形態における復号化処理の動作を説明するためのフローチャート。

【図 24】第 3 の実施形態における復号化処理の動作を説明するためのフローチャート。

【符号の説明】

10…オフィス

10-1a, 10-1n…携帯端末

10-2…無線 LAN

10-3…LAN

10-4a, 10-4n…PC

10-5…サーバコンピュータ

11…交換機

12…移動環境

20 12-1a, 12-1n…携帯端末

12-2…移动通信網基地局

12-3…移动通信網

21…CPU

22…メモリ

23…2次記憶装置

23-1…選択回路

23-1a…モードレジスタ

23-2…暗号キーレジスタ

23-3…暗号化書込回路

30 23-4…暗号データ記憶部

23-5…復号キーレジスタ

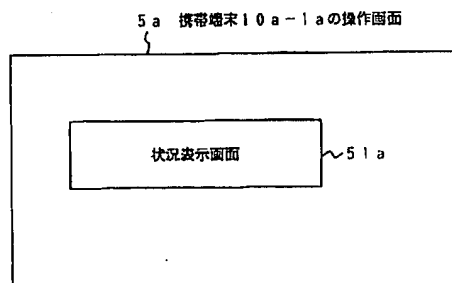
23-6…復号化読出回路

23-7…書込回路

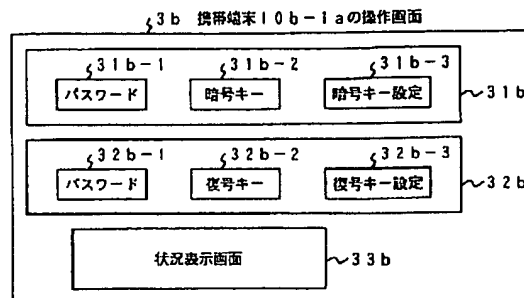
23-8…非暗号データ記憶部

23-9…読出回路

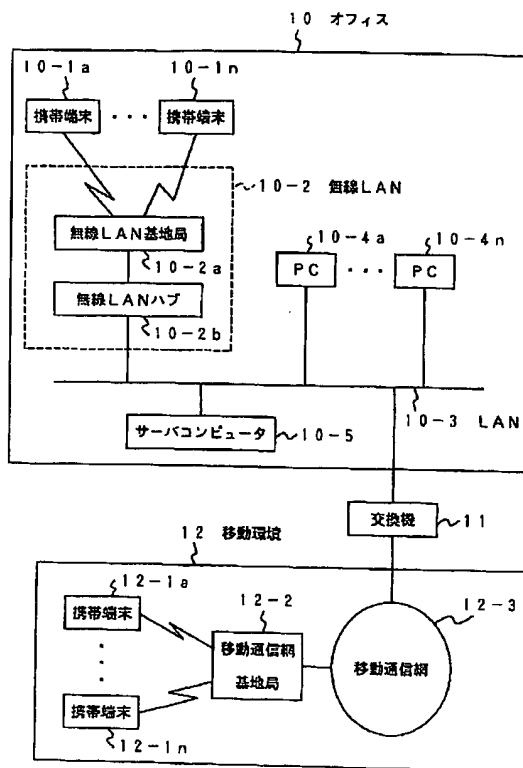
【図 12】



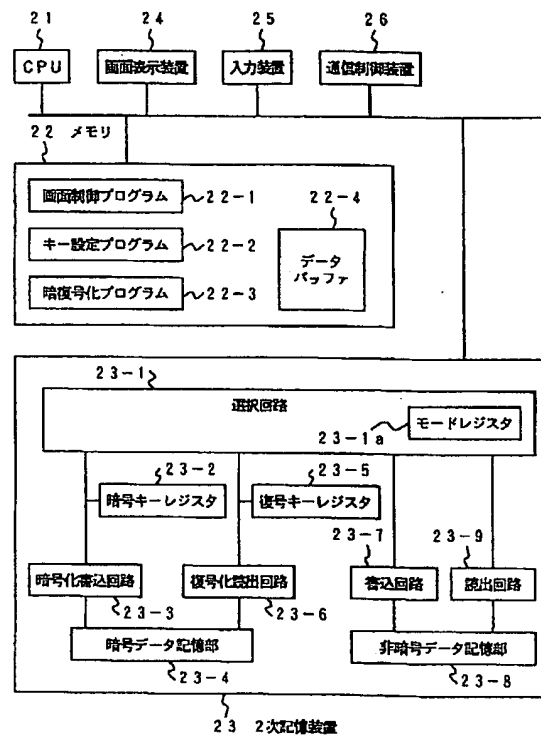
【図 19】



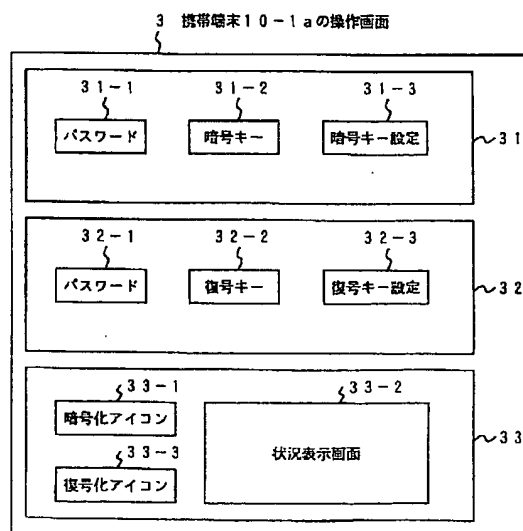
【図1】



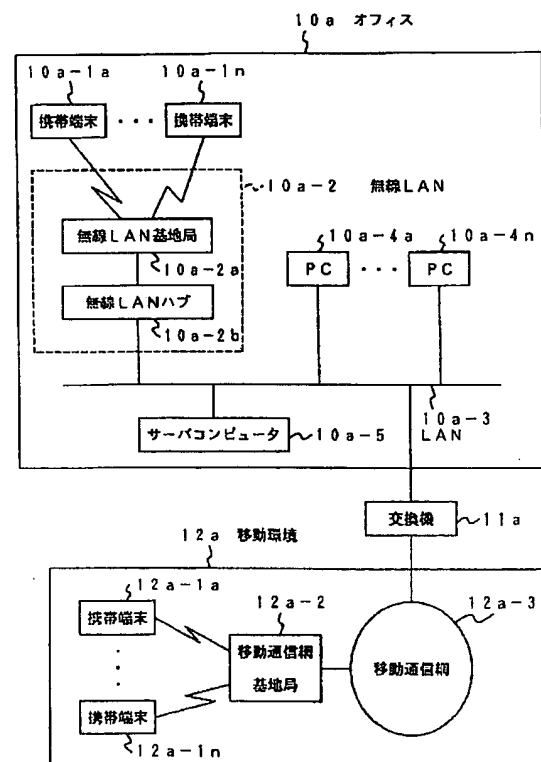
【図2】



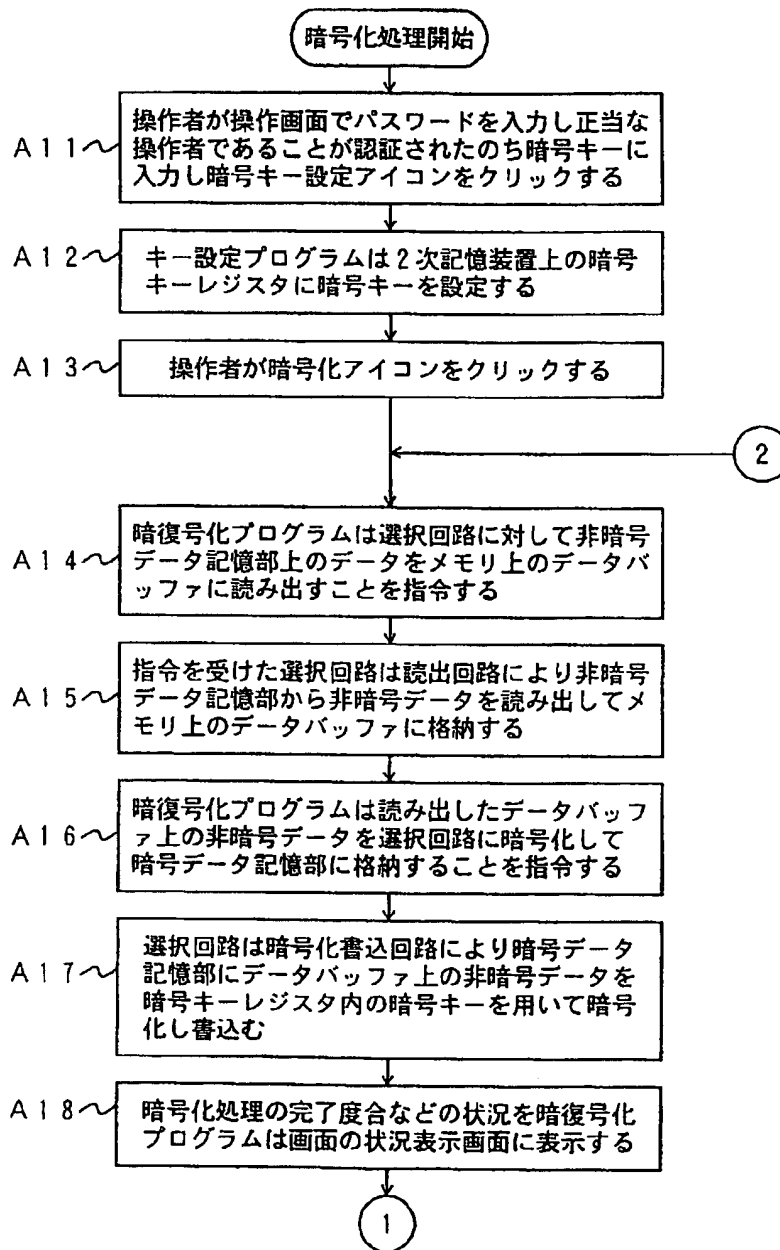
【図3】



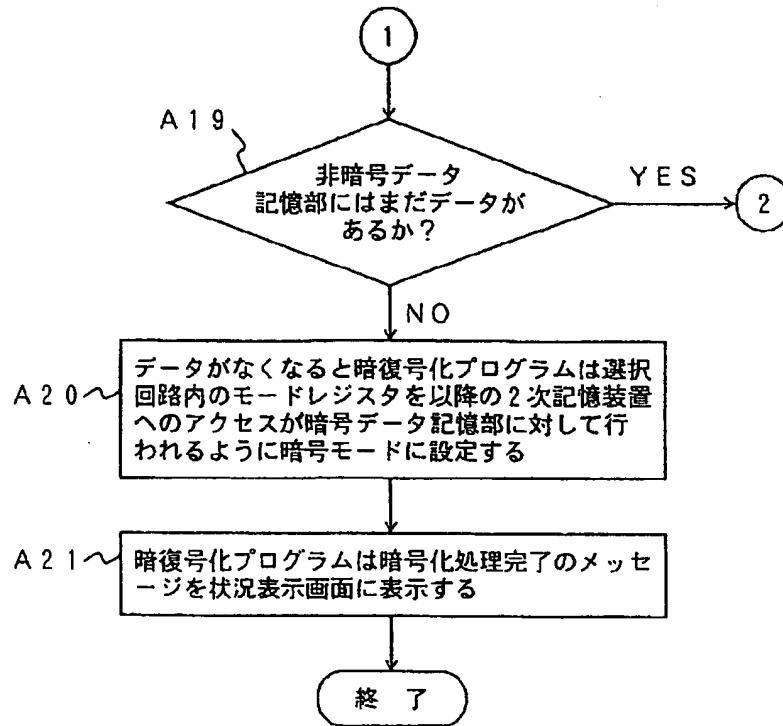
【図8】



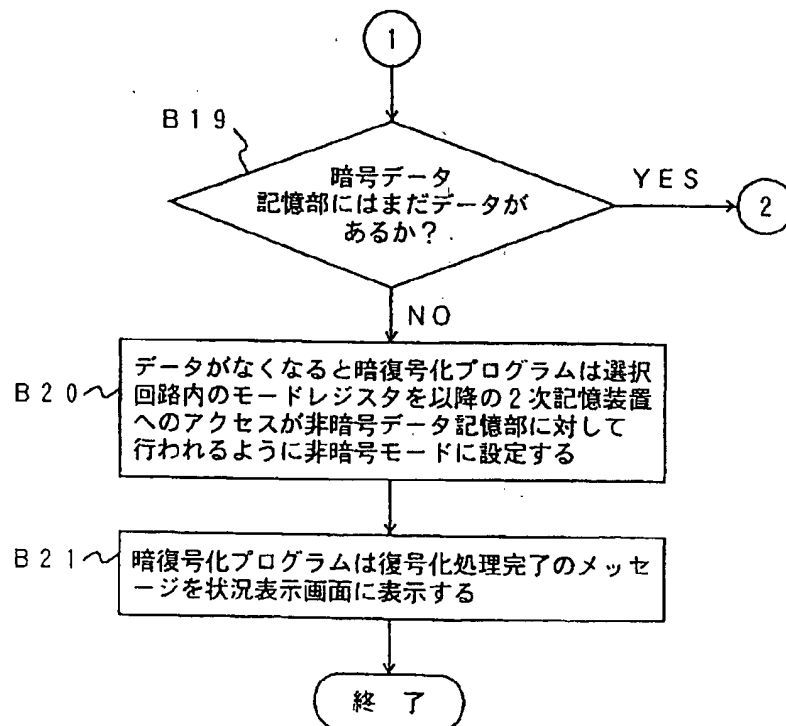
【図4】



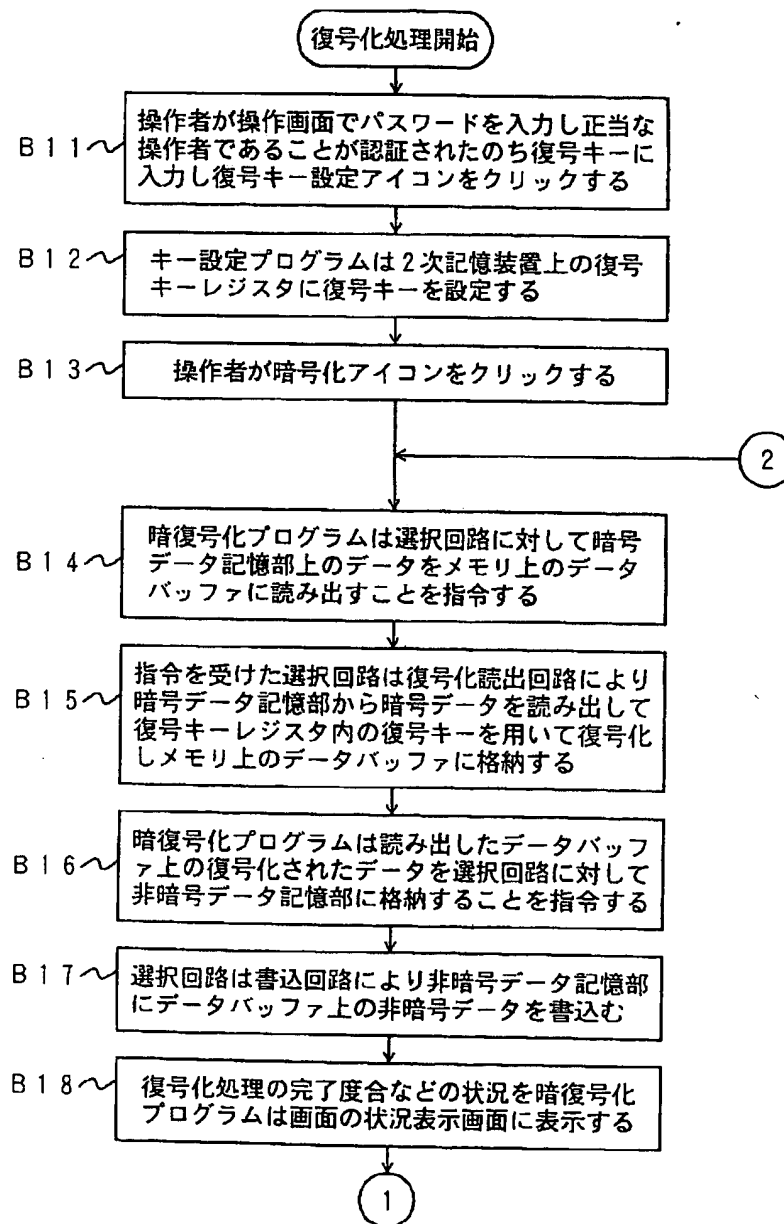
【図5】



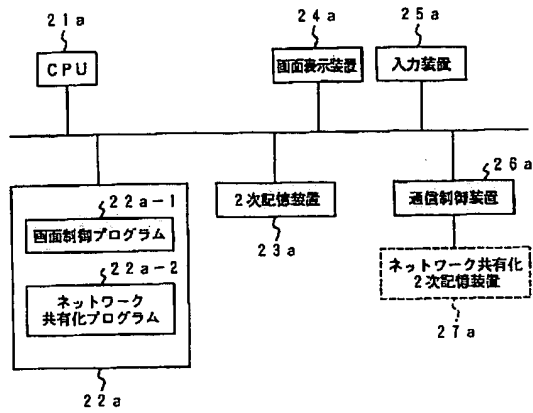
【図7】



【図6】



【図9】



【図10】

3a PC10a-4aの操作画面

ネットワーク共有化携帯端末の名前:	3a-1a	
携帯端末の操作者のユーザ識別子:	3a-1b	3a-1
携帯端末の操作者のパスワード:	3a-1c	
携帯端末の復号化キー:	3a-1d	

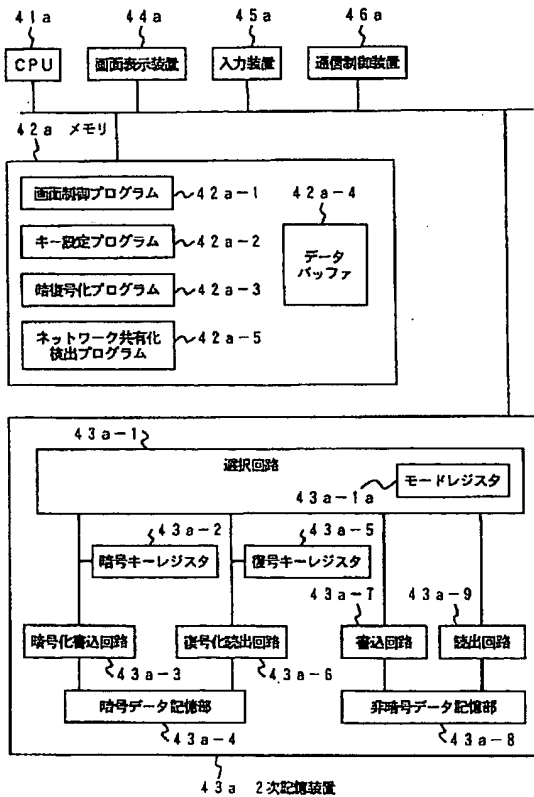
  

ネットワーク非共有化携帯端末の名前:	3a-2a	
携帯端末の操作者のユーザ識別子:	3a-2b	3a-2
携帯端末の操作者のパスワード:	3a-2c	
携帯端末の復号化キー:	3a-2d	

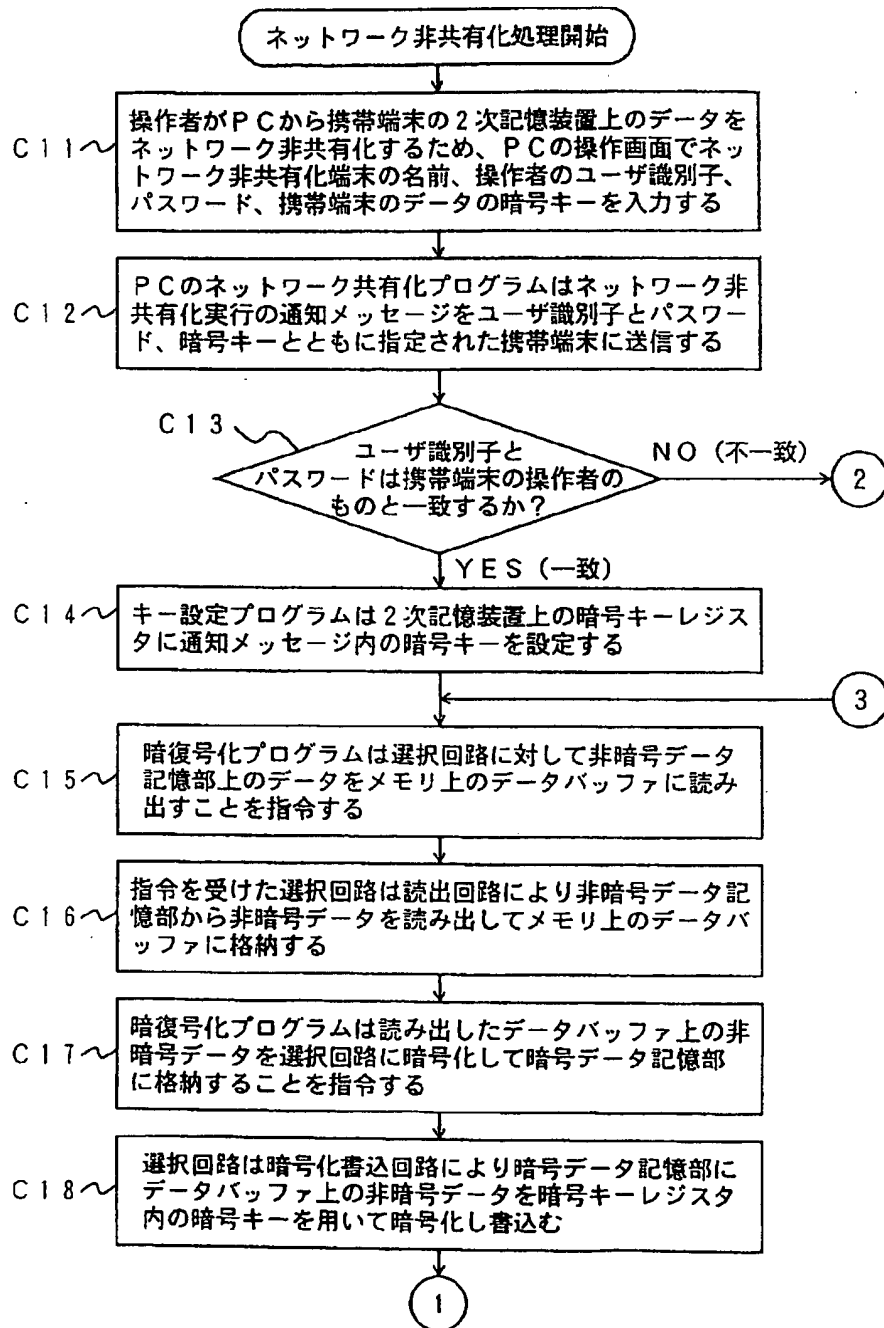
  

現在ネットワーク共有化している 携帯端末の名前:	3a-3a	3a-3
-----------------------------	-------	------

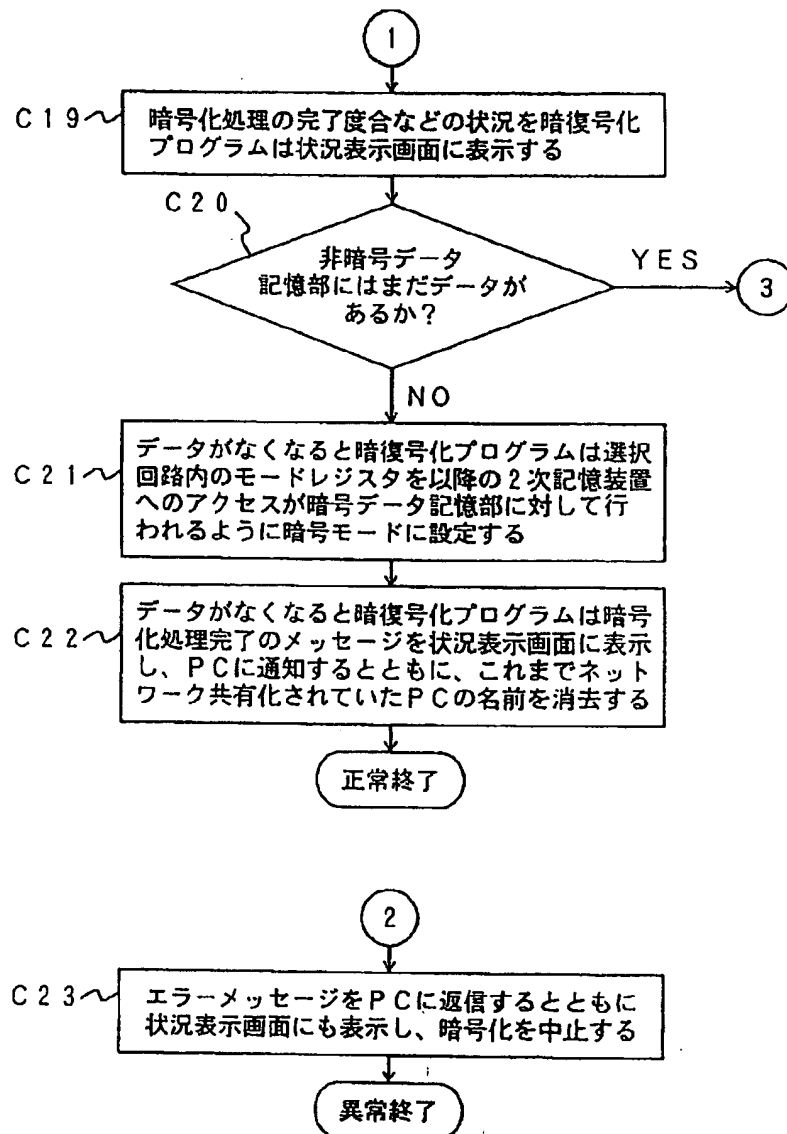
【図11】



【図13】

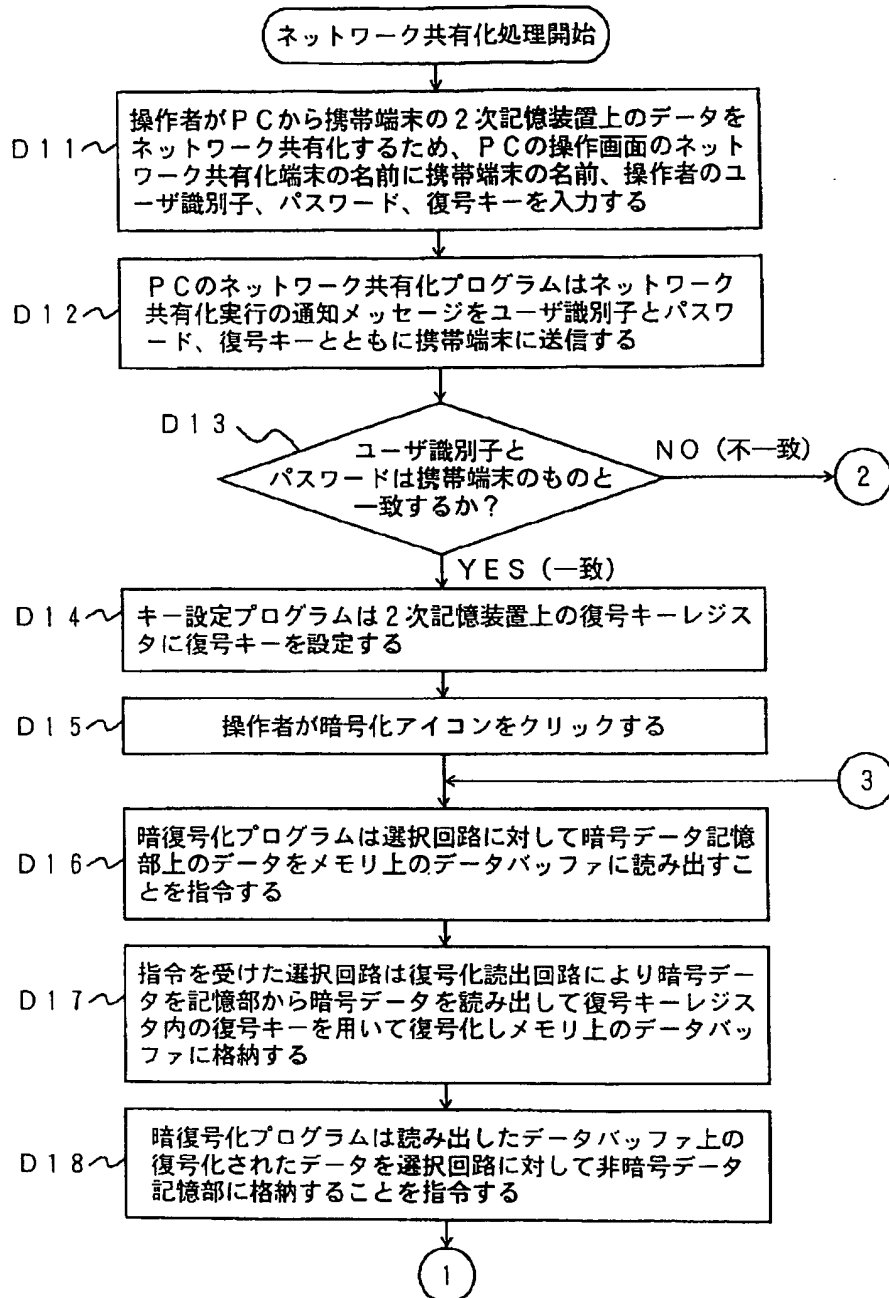


【図14】

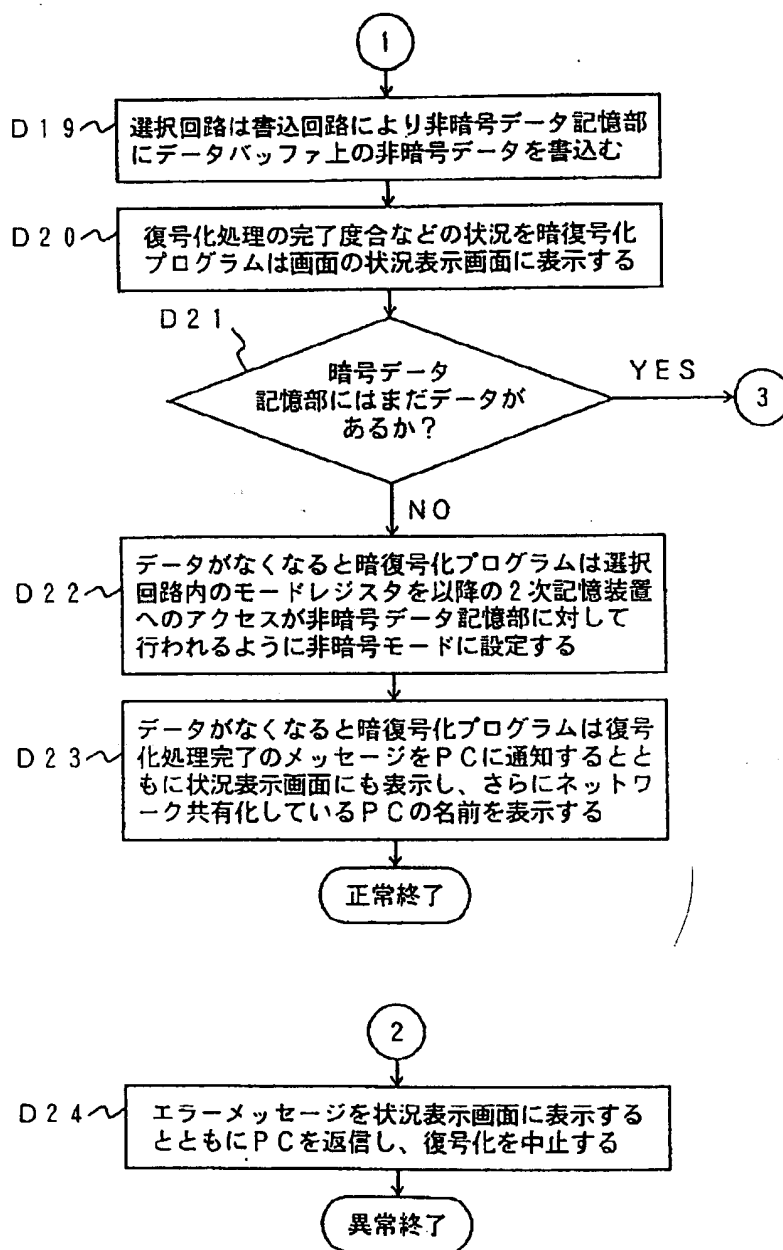




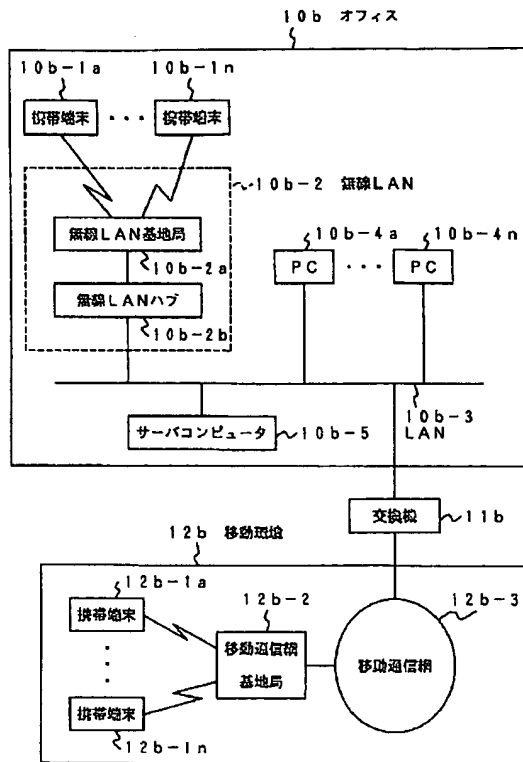
【図15】



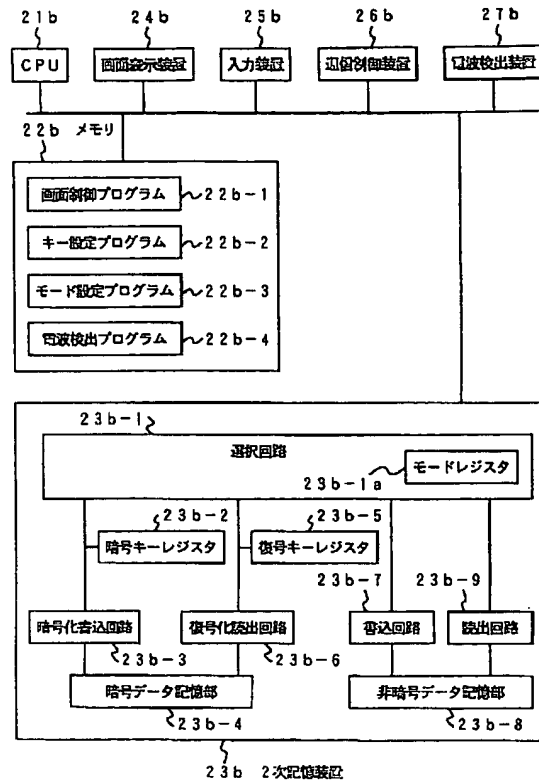
【図16】



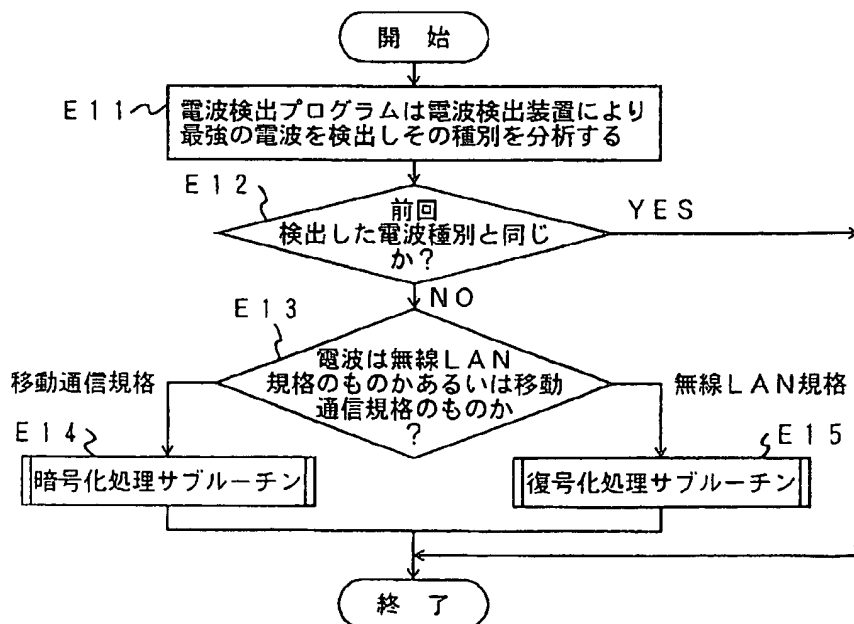
【図17】



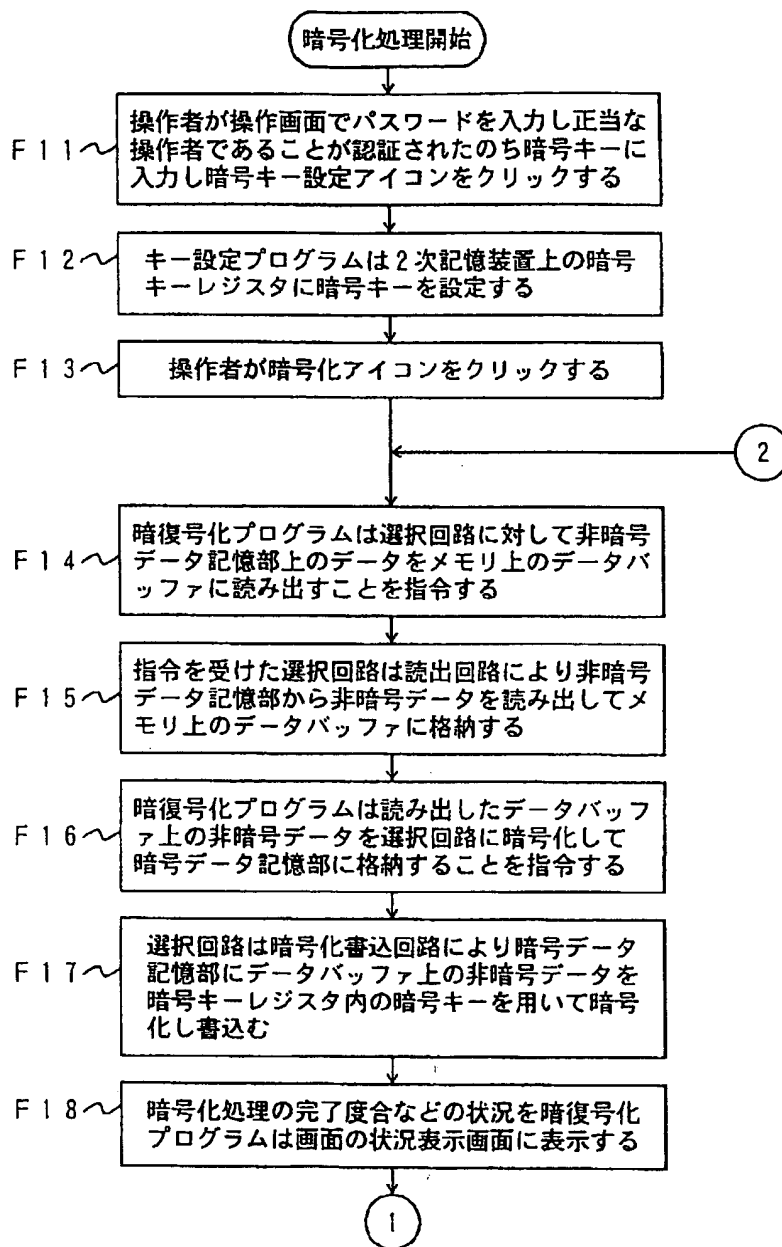
【図18】



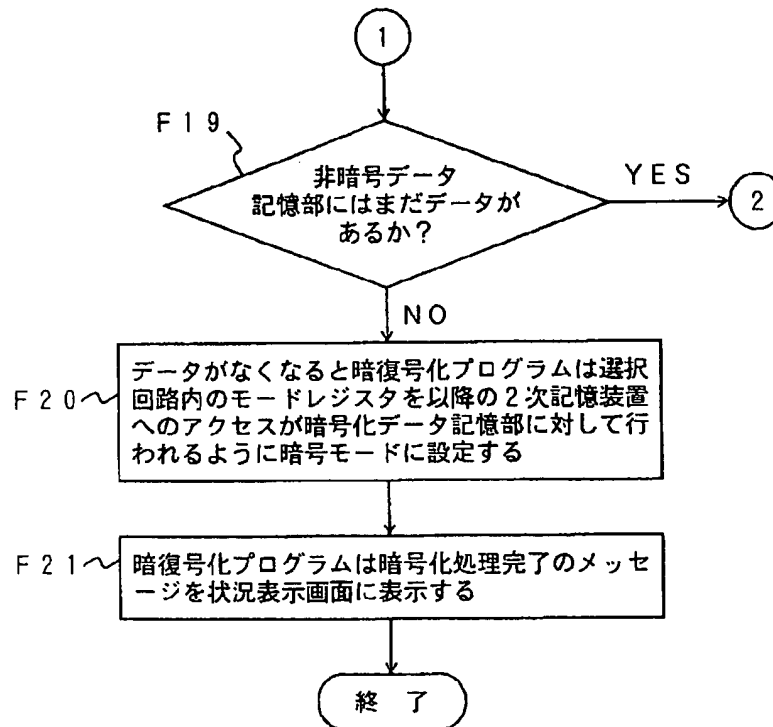
【図20】



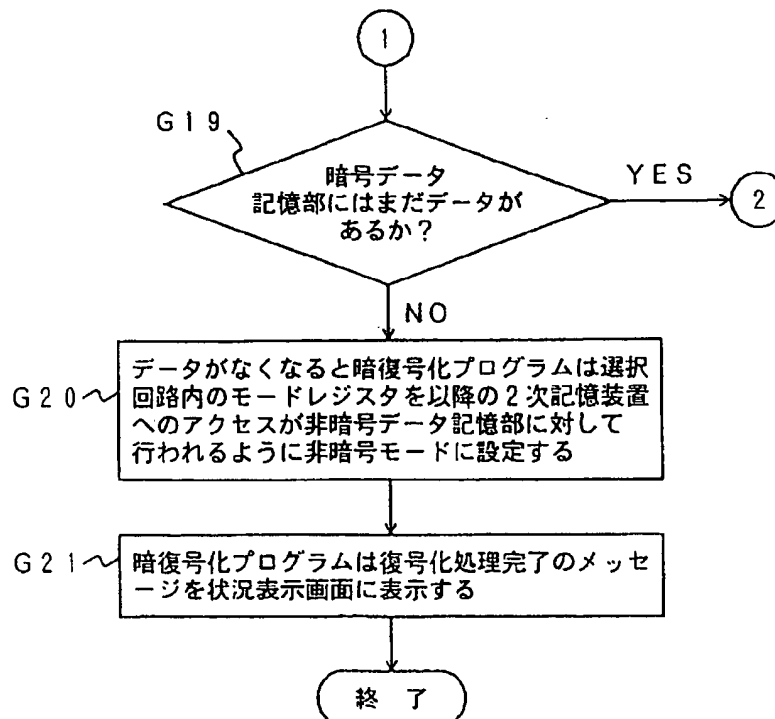
【図21】



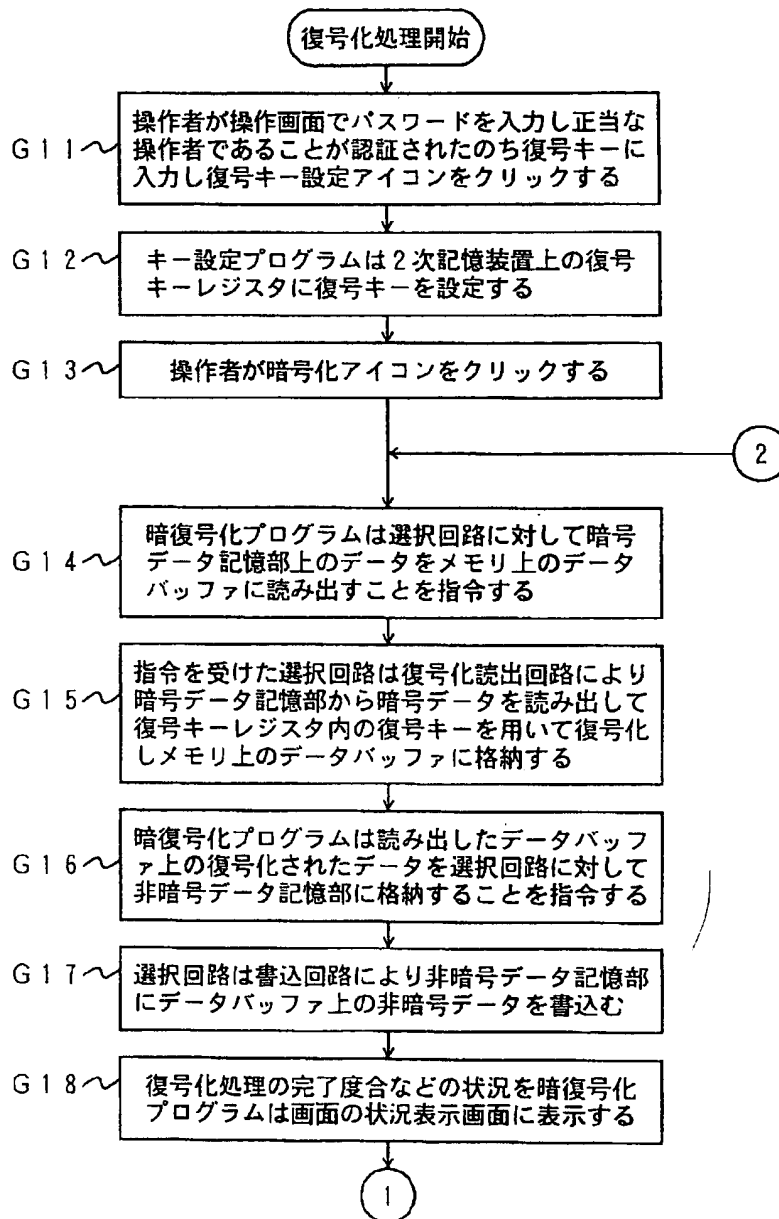
【図22】



【図24】



【図23】



フロントページの続き

(51) Int. Cl. 6

H 0 4 L 12/28

識別記号

F I

H 0 4 L 11/00

3 1 0 B

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

**This Page Blank (uspto)**